明 細 書

データクリーニング処理プログラム

技術分野

[0001] 本発明は、削除されたデータ記録媒体上のデータの復元を阻止することができるデータクリーニング処理プログラムに関するものである。

背景技術

[0002] パーソナルコンピュータ(以下、PCと記載)に用いられるデータ記録媒体には、種々のものがある。例えば、読み書き可能なデータ記録媒体として、ハードディスクやフレキシブルディスク、あるいは、CD−RW(Compact Disk ReWritable)、DVD−RAM(Digital Versatile Disc Random Access Memory)、DVD−RW(Digital Versatile Disc ReWritable)、光磁気ディスク(MO:Magneto Optical disc)などが実用されている。これらのデータ記録媒体のうち、ハードディスク以外はリムーバブルタイプである。

ハードディスクにはPC本体に内蔵可能なタイプと外付けタイプとがある。PC本体に内蔵されるタイプのハードディスクが、起動ドライブとして使用されることが多い。

[0003] 特許文献1(特開2002−041341号公報)には、ハードディスクにデータを記録する構成が開示されている。

図12は特許文献1に開示されたハードディスクの記録領域の模式図、図13は図12に示すハードディスクにファイルデータが記録される過程を示す模式図、図14は図12に示すハードディスクに記録されたファイルデータが削除される過程を示す模式図である。また、図15は、特定ソフトウェアを用いてファイルデータをハードディスクに記録する状態を示す模式図である。

[0004] 図12に示すハードディスク10は、OS(Operating System)によって複数の領域に区分して管理されている。すなわち、ハードディスク10の内部は、OSによって、MBR(Master Boot Record)領域11、BPB(BIOS Parameter Block)領域12、FAT(File Allocation Table)領域13、ディレクトリ領域16及びデータ領域17に区分されている。

[0005] MBR領域11は、OSの起動プログラム(OS Boot Loader)や、そのパーティション位

置、サイズなどの位置情報であるパーティションテーブルが格納される領域である。BPB領域12は、周辺機器との入出力を管理するためのFATやディレクトリエントリに関するデータであるBIOSパラメータが格納される領域である。

[0006] FAT領域13は、FAT14及びそのコピーであるFAT15が格納される領域である。FAT14は、図13(a)のように、アドレスデータを記録可能な複数の記録領域14aで形成され、各記録領域14aにはデータ領域17のクラスタアドレスに対応させて00H, 01H, 02Hのアドレスが付されている。FAT15もFAT14と同一の記録領域で形成され、FAT14のデータが破壊した場合のバックアップ動作を行う。なお、図13, 図14では、説明の便宜上、FAT14の記録領域14a及びデータ領域17のクラスタ17aには16進2バイトのアドレスが付されるものとしている。

[0007] 図13(a)に示すように、FAT14の記録領域14aのうち、開放符号「00H」が記録された記録領域14aは空き領域を示す。また、01H以降のアドレスが記録されている記録領域14aは、データ領域17のクラスタ17aにデータが記録されている領域を示す。例えば、図13(a)に示すように、FAT14のアドレス01Hの記録領域14aにアドレス03Hが記録されているときは、データ領域17のアドレス01Hのクラスタにファイルデータが記録され、そのファイルデータに連続するデータがアドレス03Hのクラスタに記録されることを示す。すなわち、FAT14の記録領域14aに記録されるアドレスは、ファイルデータが記録されるデータ領域17のチェーンクラスタアドレスを示している。又、ファイルの終端部を記録したデータ領域17のクラスタ17aに対応するFAT14の記録領域14aには、ファイル終端符号である「FFH」が記録される。

[0008] ディレクトリ領域16は、ファイル情報が記録される領域である。図13(c)に示すように、ディレクトリ領域16には、ハードディスク10に記録されるファイル毎に、ファイル名、ディレクトリ名、拡張子、作成日時、最終更新日時、ファイルサイズ、エントリアドレス、属性などのファイルに関する情報が記録される。

[0009] また、データ領域17は、ファイルデータ本体が記録される領域である。図13(e)に示すように、データ領域17は、データを記録する複数のクラスタ17aで構成されている。各クラスタ17aには00H, 01H, 02H等 のアドレスが付されている。

[0010] テキストエディタやワープロなどのソフトウェアで作成したデータを、ハードディスク1

0に保存する場合は、OSによって図13に示す処理が実行される。

図13には、ワープロで作成された「XYZ」ファイルが記録されているハードディスク10に、テキストエディタで作成されたファイル「ABC」を保存する場合の例が示されている。

OSは、まず図13(a)に示すFAT14を参照して、開放符号「00H」が記録されている空き記録領域14aのうち、アドレス00Hを除く最もアドレスの小さい記録領域14aであるアドレス02Hを求める。そして、OSは、図13(e)に示すデータ領域17のアドレス02Hのクラスタ17aにデータを記録する。

[0011] ファイル「ABC」の大きさが、一つのクラスタ17aの容量を超える場合には、OSはFAT14を参照して、アドレス02Hの次に小さい空き記録領域であるアドレス05Hを求める。そして、アドレス05Hをアドレス02Hの記録領域14aに記録すると共に、データ領域17のアドレス05Hのクラスタ17aに、続きのデータを記録する。このように、OSは、FAT領域13の空いている複数の記録領域14aに対応するデータ領域17の複数のクラスタ17aにデータを記録する。データの終端部が記録されるアドレス15Hの記録領域14aには、ファイル終端符号である「FFH」を記録する。

[0012] 続いて、OSは、図13(d)に示すように、ハードディスク10のディレクトリ領域16に、ファイル名「ABC」、保存先のディレクトリ名、拡張子「TXT」、作成日時、最終更新日時、ファイルサイズ「005」、エントリアドレス「02H」及び属性を記録してデータの保存処理を完了する。

[0013] 又、ファイル「ABC」にアクセスされると、OSは、図13(d)に示すディレクトリ領域16を参照してファイル「ABC」のエントリアドレス「02H」を求める。そしてOSは、図13(b)に示すFAT14を参照してファイル「ABC」のデータが記録されたチェーンクラスタアドレスを求め、データ領域17から当該ファイルを、メインメモリ領域に読み込む。メインメモリ領域は、中央処理装置(CPU)で管理されている。

[0014] 一方、テキストエディタやワープロソフトなどのソフトウェア、あるいは、OSによって、ファイルデータをハードディスク上から削除する場合には、図14に示す処理が実行される。

すなわち、図14(c)、(d)に示すように、ハードディスク10上のファイル「XYZ」を削

除する場合には、OSは、ディレクトリ領域16を参照してファイル「XYZ」のエントリアドレス01Hを求める。そして、図14(b)に示すように、アドレス01Hの記録領域14aに記録されたチェーンクラスタのアドレス「03H」(図14(a)に示す)に、開放符号「00H」を上書きする。続いて、アドレス03Hの記録領域14aに記録されたチェーンクラスタのアドレス「04H」(図14(a)に示す)に開放符号「00H」を上書きする。

このように、ファイル「XYZ」に係るFAT14の全ての記録領域14aに開放符号「00H」を上書きする。なお、図14(b)では、FAT14のアドレス01Hと16Hにのみ引き出し線を使用して「00H」を記載してあり、その他のファイル「XYZ」に係るアドレスへの開放符号「00H」の記載は省略している。この後、OSは、図14(d)に示すように、ディレクトリ領域16のファイル「XYZ」に係るデータを消去し、ハードディスク10上のファイル「XYZ」の削除処理を完了する。

[0015] 以上を要約すると次のとおりとなる。

オペレータが、ファイル「XYZ」を削除操作すると、ファイル「XYZ」のデータ本体が記録されていたデータ領域17のクラスタ17aのアドレスに対応するFAT14の記録領域14aがOSによって開放される。

[0016] 開放された記録領域14aに対応するデータ領域17のクラスタ17aには、別のデータの上書き保存が可能になる。すなわち、オペレータがファイル「XYZ」の削除操作を行っても、データ領域17のクラスタ17aに記録されたデータ本体は消去されず、データ本体のインデックスに相当するFAT14の記録領域14aが開放されるだけである。

[0017] すなわち、記録媒体をMS−DOS(米国 Microsoft Corporationの米国及びその他の国における登録商標又は商標)などのオペレーティングシステム(以下、OSと記載)による削除操作(物理フォーマットや論理フォーマットを施すなど)しただけでは記録されたデータ本体は消去されない。

[0018] 従って、ファイル「XYZ」を削除した後は、当該クラスタ17aに別のファイルデータが上書きされるまでは、ファイル「XYZ」のデータ本体が残存したままとなる。

特許文献1:特開2002−041341号公報

発明の開示

発明が解決しようとする課題

[0019] PCを手放す際(他人に譲る、下取りに出す、又は破棄するなど)には、記録媒体に記録されたデータを予め削除しておき、削除したデータが復元されないようにすることが好ましい。PCを手放す前に、データを削除するという操作は一般的に行われているが、上記の事情により、削除したデータが、第三者によって復元されてしまう恐れがある。

[0020] 特に、ハードディスクは他のリムーバブルなデータ記録媒体と異なり、PC本体に固定されたものが多く、一般にハードディスク自体を持ち運ぶことはできない。このため、ファイルの削除処理を行っているにも拘わらず、削除したデータが第三者によって復元され、データが漏洩する恐れがあった。

[0021] この問題を解決するべく、記録媒体に記録されたデータ本体をOS上で動作するデータクリーニングソフトウェアが開発されている。このソフトウェアは、記録媒体に任意のダミーデータを上書きして元のデータを削除するものである。

[0022] また、このようなOSによるファイル管理の問題に関連して、コンピュータにインストールされる特定ソフトウェアでは、データ領域の一部をソフトウェア管理領域として確保するものがある。そして、このような特定ソフトウェアでは、特定ソフトウェアで作成したファイルの保存処理を行うと、更新データを旧データと区分してデータ領域に記録すると共に、当該ファイルに係る更新データ及び全ての旧データを記録したクラスタアドレスを示すFATデータをソフトウェア管理領域に記録する処理を行う。

[0023] すなわち、このような特定ソフトウェアでは、図15(a)に示すように、ハードディスク10のデータ領域17に特定ソフトウェア(プログラム)18を格納すると、当該ソフトウェア18は、OSの管理下において所定サイズのソフトウェア管理領域19をデータ領域17上に確保する。

[0024] そして、当該特定ソフトウェア18で作成したファイル「No. 1」の保存処理を行うと、図15(a)に示すように、データ領域17に「No. 1」ファイルデータ30が記録される。更に、OSで管理されるFAT14とは別に、当該特定ソフトウェア18によってファイル「No. 1」のFATデータ30aがソフトウェア管理領域19に記録される。当該特定ソフトウェア18で作成した別のファイル「No. 2」の保存処理を行う場合にも同様の処理が行わ

れる。

[0025] また、特定ソフトウェア18で作成したファイル「No. 1」の更新保存処理を行うと、図15(b)に示すように、最新の更新データ30が記録されると共に、更新前の旧データ31が更新データ30とは別のクラスタに記録される。更に、更新データ30及び旧データ31の各々のFATデータ30a, 31aがソフトウェア管理領域19に記録される。更新保存処理を繰り返すと、更新データ30及び旧データ31に加えて旧々データ32が記録され、ソフトウェア管理領域19に更新データ30、旧データ31及び旧々データ32のFATデータ30a, 31a, 32aを記録する処理が行われる。

但し、OSは、特定ソフトウェア18によって記録されたデータのうち、更新データ30, 35のみを管理しており、旧データ31, 36や旧々データ32の記録されたクラスタに対応するFATは開放されている。

[0026] 更に、特定ソフトウェア18で作成したファイルの削除処理を行うと、OSによって更新データ30, 35の記録されたクラスタに対応するFATは開放されるが、削除処理によっても、ソフトウェア領域19に記録された各ファイルのFATデータ30a, 31a, 32a及びFATデータ35a, 36aはそのまま残存する。

[0027] すなわち、このような特定ソフトウェア18は、ファイルの更新処理を行うと、旧データや旧々データの記録されたFATデータがソフトウェア管理領域19に残存したままとなる。又、ファイルの削除処理を実行しても、当該ファイルに係るデータが記録された全てのクラスタを示すFATデータがソフトウェア管理領域19に残存したままとなる。

また、開放されたクラスタに別のデータが上書きされるまでは、データ領域17のデータ本体も残存したままとなる。

[0028] このため、このような特定ソフトウェアを使用する場合、ユーザーがファイルの更新処理を行ったつもりでも、特殊なソフトウェアによってソフトウェア管理領域19に記録されたFATデータを参照して、旧データ31や旧々データ32を復活して読み取られる恐れがあった。また、削除処理を行っても、特殊なソフトウェアによって更新データ30や旧データ31, 旧々データ32を復元され、復元されたデータが漏洩する恐れがあった。このため、セキュリティの確保の面から改善が望まれていた。

[0029] さらに、近時、内蔵型ハードディスクにBIOSなどで管理する隠し領域を設け、当該

隠し領域にOSのインストール機能を搭載したハードディスクが開発されており、このようなハードディスクを備えたPCが提供されている。

[0030] このようなPCでは、CD−ROM等で提供されるリカバリーディスクを使用することなくOSの再インストールができ、省コスト化が図られると共に、リカバリーディスクを保管管理する必要もなく便利である。

[0031] しかし、従来のクリーニングソフトウェアは、ハードディスク内の所望するデータだけを選択的に消去することができない。

つまり、OSのインストール機能を備えたハードディスクに対して、従来のクリーニングソフトウェアを用いてデータクリーニング処理を行うと、BIOSで管理される隠し領域までもが上書きされてしまう。このため、ハードディスクに記録された削除済みのデータは復元できなくなるものの、OSのインストール機能までが使用不能となってしまう。

一方、各PCメーカは、ハードディスクにOSをインストールするための機能を持たせる代わりに、CD−ROM等のリカバリーディスクを添付せず、コスト削減を図っている。従って、従来のクリーニングソフトウェアでハードディスクのデータクリーニング処理を行うと、当該ハードディスクを、購入当初の環境に戻すことができなくなってしまう。

[0032] 本発明は、上記問題に鑑みて提案されるものである。

すなわち本発明は、データ記録媒体に残存する削除済みのデータを復元できないようにするデータクリーニング処理プログラムを提供することを第一の目的としている。

[0033] さらに本発明は、データ記録媒体に格納されたデータを選択的に消去可能にすることにより、残存する削除済みデータの復元を阻止し、且つ、データ記録媒体を容易に購入当初の状態に復元させることのできるデータクリーニング処理プログラムを提供することを第二の目的としている。

課題を解決するための手段

[0034] 前記二つの目的を達成するために、本発明者らは以下の技術的手段を講じた。

[0035] 以下に記述するOS(Operating System)とは、本発明のデータクリーニング処理プログラムやアプリケーションソフトウェアを動作させる基本プログラムを指す。OSには、例えば、Windows(米国 Microsoft Corporationの米国及びその他の国における登録商標又は商標)やMS−DOSあるいはMacOS(米国その他の国々で登録された

Apple Computer, Inc.の登録商標)などがある。

[0036] 制御手段とは、OSと、当該OSによってデータ記録媒体へのアクセス制御を実行する中央処理装置(CPU)とを含んだ構成を指す。また、以下の説明において、FAT領域とは、少なくとも、データ本体を記録したデータ領域のクラスタアドレスを管理するFAT(File Allocation Table)が格納される領域を指す。FAT領域は、FATに加えて、ファイル情報に係るディレクトリデータやデータの一部が格納される構成であっても良い。また、以下の説明において、チェーンクラスタアドレスの終端には、データの終端部を示すファイル終端符号が記録されるものとする。

[0037] BIOS(Basic Input/Output System)とは、データ処理装置(PC)に接続される各種のディスクドライブやキーボードなどの周辺機器に対する基本的な入出力制御をOSやアプリケーションソフトウェアに対して提供するプログラムを指す。BIOSは、通常、データ処理装置の不揮発性メモリに記憶される。

[0038] さらに、メインメモリとは、制御手段から直接アクセスが可能なメモリである。メインメモリは、プログラムファイルやデータを読み込んで実行する。

[0039] 前記第一の目的を達成するための本発明は、データ記録媒体と、当該データ記録媒体へのアクセス制御を行う制御手段とを備えたデータ処理装置に格納されるデータクリーニング処理プログラムであって、データ記録媒体は、ファイルデータを記録する複数のクラスタを有しファイルデータを1又は2以上のクラスタに分散して記録するデータ領域と、クラスタを特定するアドレスの付された複数の記録領域を有し、各記録領域に対応するクラスタに記録されたファイルデータに連続するデータの記録されたチェーンクラスタのアドレス又は開放符号のいずれかを各記録領域毎に記録するFAT領域とに区分して制御手段で管理され、FAT領域を参照して、開放符号が記録された全ての記録領域のアドレスを抽出し、抽出したアドレスに対応するクラスタに所定データを順次上書きする処理を行う。

[0040] ここで、FATを構成する複数の記録領域のうちの、ある一つのデータに関連するチェーンクラスタアドレスが記録された記録領域のアドレスに対応するデータ領域のクラスタは、OSで管理されるデータ(削除操作されていないデータ)が記録されたクラスタである。

[0041] 逆に、過去に一度もデータが記録されたことがないクラスタや、削除処理や更新処理された結果、OSの管理が不要になったデータが残存するクラスタに対応するFAT領域の記録領域のアドレスには、開放符号が記録される。

[0042] 本発明によれば、FAT領域を構成する複数の記録領域のうちの、開放符号が記録された記録領域のアドレスに対応するデータ領域のクラスタに、所定データを上書きする。すなわち、削除処理や更新処理によって生じた管理不要なデータが残存する全てのクラスタに所定データが上書きされる。

[0043] これにより、特殊な解析ソフトウェアでFAT領域やデータ領域を参照しても、削除処理や更新処理されたデータに係る全ての旧データの復元が不可能となる。よって、データの漏洩を阻止することが可能となる。

[0044] 本発明は、データ記録媒体と、当該データ記録媒体へのアクセス制御を行う制御手段とを備えたデータ処理装置に格納されるデータクリーニング処理プログラムであって、データ記録媒体は、ファイルデータを記録する複数のクラスタを有しファイルデータを1又は2以上のクラスタに分散して記録するデータ領域と、クラスタを特定するアドレスの付された複数の記録領域を有し、各記録領域に対応するクラスタに記録されたファイルデータに連続するデータの記録されたチェーンクラスタのアドレス又は開放符号のいずれかを各記録領域毎に記録するFAT領域とに区分して制御手段で管理されると共に、データ領域には特定ソフトウェアが格納され、特定ソフトウェアは、データ領域の一部をソフトウェア管理領域として確保すると共に、作成したファイルの保存時には、更新ファイルデータを旧データと区分してデータ領域に記録し、更に、当該ファイルに係る更新データ及び全ての旧データを記録したクラスタを示すFATデータをソフトウェア管理領域に記録する構成とされ、特定ソフトウェアで作成したファイルを指定し、ソフトウェア管理領域に記録されたFATデータを参照して当該ファイルに係るデータが記録された全てのクラスタアドレスを抽出すると共に、FAT領域を参照して開放符号が記録された全ての記録領域のアドレスを抽出し、抽出した双方のアドレスの論理積アドレスに対応するクラスタに所定データを順次上書きする処理を行う。

[0045] 本発明では、特定ソフトウェアによって記録されたソフトウェア管理領域のFATデー

タを参照することにより、指定されたファイルに係るデータが記録された全てのクラスタアドレスを抽出する。すなわち、ソフトウェア管理領域のFATデータを参照することにより、当該ファイルの更新データ(最新データ)及び全ての旧データが記録されたクラスタアドレスを抽出する。

[0046] また、制御手段は、FAT領域を参照して開放符号が記録された記録領域のアドレスを全て抽出する。すなわち、OSによって管理されているファイルデータが記録されたクラスタ以外の、管理不要なデータが残存する全てのクラスタに対応するアドレスを抽出する。

[0047] そして、制御手段は、抽出した双方のアドレスの論理積を演算することにより、指定されたファイルの全てのデータに係るクラスタのうちの、OSで管理されているファイルデータが記録されていないクラスタにのみ所定データを上書きする。

[0048] 従って、データクリーニング処理の実行前に、指定されたファイルの削除処理が実行されている場合には、当該ファイルに係る全てのクラスタに上書きが行われる。また、データクリーニング処理の実行前に、当該ファイルの更新処理が行われている場合は、更新データ(最新データ)を除く全ての旧データに係るクラスタに所定データの上書きが行われる。

[0049] すなわち、本発明によれば、OSで管理されている必要なファイルが記録されたクラスタを除いて、指定されたファイルに係るデータが残存するクラスタにのみ所定データが上書きされる。これにより、ソフトウェア管理領域に記録されたFATデータを特殊なソフトウェアで参照し、削除されたファイルや更新されたファイルの復元を阻止することが可能となる。

[0050] また、本発明では、指定されたファイルに係るデータが記録されたクラスタのうち、OSで管理されているファイルデータが記録されているクラスタを除くクラスタにのみ所定データが上書きされる。

従って、指定されたファイルのデータクリーニング処理を短時間に完了することが可能である。

すなわち、本発明では、特定ソフトウェアにおける更新データや旧データの復活を阻止することができ、データ記録媒体のセキュリティを確実に確保できるデータクリー

ニング処理プログラムを提供できる。

[0051] 本発明のデータクリーニング処理プログラムは、前述の構成に加えて、ソフトウェア管理領域に記録されたFATデータのうち、上書き処理が行われたクラスタに対応するFATデータに所定データを上書きする処理を行うことが好ましい。

[0052] ここで、本発明によれば、指定されたファイルに係るデータが記録されたクラスタに上書き処理が行われる。従って、指定されたファイルに係るFATデータが特定ソフトウェアで管理されるソフトウェア管理領域に残存したままであってもデータの復活は阻止される。

[0053] しかし、特殊なソフトウェアでFATデータが参照され、削除処理したデータが記録されたていたクラスタが特定されると、当該クラスタの残留磁気を解析するなどの方法によって削除処理したデータが復元される可能性が生じる。

本発明によれば、ソフトウェア管理領域に残存するFATデータも所定データで上書き処理するので、削除処置したデータが記録されていたクラスタの特定を阻止することができる。これにより、削除処置したデータの復元を完全に阻止することができ、セキュリティを一層向上させることが可能となる。

すなわち、本発明によれば、特定ソフトウェアの記録するFATデータの読み取りを阻止することができ、データ記録媒体のセキュリティを一層確保可能なデータクリーニング処理プログラムを提供できる。

[0054] 本発明は、制御手段によって前述のいずれかの処理プログラムを選択的に実行可能なデータクリーニング処理プログラムである。

[0055] 本発明によれば、必要に応じて任意に処理プログラムを選択して実行することにより、必要に応じて削除処理したデータが記録されていたクラスタへの上書き処理を効率良く行うことが可能となる。

すなわち、本発明によれば、前述の発明のデータクリーニング処理プログラムの奏する効果を兼ね備えたデータクリーニング処理プログラムを提供できる。

[0056] 本発明のデータクリーニング処理プログラムは、前述の構成に加えて、所定データの上書きが、同一のデータ又は異なるデータを、任意の所定回数だけ繰り返して上書きする構成としてもよい。

[0057] ここで、ハードディスクやフレキシブルディスクなどの磁気データ記録媒体では、媒体が磁化される磁極を所定の閾値で仕切ることによって「1」,「0」の判別を行うデータ記録方式が採用される。ところが、「1」が記録された部位に「0」を上書きすると、「0」の読み出しは行われるものの、磁極は完全には反転していない。従って、磁化レベルを詳細に解析する特殊処理が行われると、所定データを上書きしているにも拘わらず、上書き前のデータが復元される可能性が生じる。

[0058] 本発明では、ソフトウェアによってデータ領域のクラスタや、ソフトウェア管理領域のFATデータに繰り返し同一の所定データ又は異なる所定データを上書き処理する。これにより、磁化の履歴をたどることによるデータ本体の復元や、データ本体のインデックスに相当するFATデータの復元が極めて困難になり、データの読み取りを効果的に阻止することが可能となる。

[0059] 上書きする所定データは、例えば、「00H」や「FFH」あるいは「E5H」などの任意のデータとすることができる。これらのうちのいずれか一つの所定データ又は複数の所定データを任意の回数だけ繰り返しクラスタに上書きすることにより、データの読み取りを完全に阻止することが可能となる。

すなわち、本発明によれば、上書きしたデータの読み取りを完全に阻止することができ、データ記録媒体のセキュリティを一層確保することのできるデータクリーニング処理プログラムを提供できる。

[0060] 本発明のデータクリーニング処理プログラムには、データ記録媒体としてハードディスクを採用するのが好ましい。

[0061] 前記した本発明のデータクリーニング処理プログラムは、FAT領域とデータ領域とに区分して管理されるデータ記録媒体、すなわち、ハードディスクやフレキシブルディスク、CD−RW、DVD−RAM、DVD−RW、及びMO(光磁気ディスク)などのデータ記録媒体の全てに適用することが可能である。

[0062] ハードディスクを除く他のデータ記録媒体は全てリムーバブルな媒体である。ハードディスクはコンピュータ本体に固定的に搭載されることが多い。従って、リムーバブルな媒体に比べてハードディスクは、削除処理を行ったファイルデータや、更新処理を行ったファイルの旧データが無断で読み出される不具合が生じ易い。

[0063] しかし、削除処理を施したデータがハードディスク上に残存していても、本発明のデータクリーニング処理を実施することにより、削除処理を施したデータの復元を阻止することができる。従って、データの漏洩を阻止することができ、セキュリティを確保することが可能となる。

すなわち、本発明によれば、ハードディスクのセキュリティを確保することのできるデータクリーニング処理プログラムを提供できる。

[0064] 本発明のデータクリーニング処理プログラムは、前述の構成に加えて、予め定められた時刻に至ったとき、又は、他の処理が所定時間継続して行われないときに、制御手段によって自動的に起動されてクリーニング処理を開始する構成とすることができる。

[0065] ここで、本発明のデータクリーニング処理は、削除処理済みの不要なデータが残存するクラスタに所定データを上書きする。このため、記録容量が大きいデータ記録媒体ほど、所定データの上書きに要する時間が増大する。そこで、データ処理装置(PC)を使用しないときにデータクリーニング処理を行わせるのが効率的である。さらに、データクリーニング処理を自動的に実行すると、手間も軽減される。

[0066] 本発明によれば、データ処理装置を使用しない深夜などにデータクリーニング処理の開始時刻を設定し、データクリーニング処理を効率的に行うことが可能となる。また、データ処理装置が使用されていない時間帯を他の処理(ワードプロセッサによる文書の作成等)が所定時間継続して行われないことによって判別し、クリーニング処理を開始させることができる。これにより、中央処理装置(CPU)への負担を軽減しつつ効率良くクリーニング処理を行うことが可能となる。

すなわち、本発明によれば、データ記録媒体のデータクリーニング処理を効率良く行うことのできるデータクリーニング処理プログラムを提供できる。

[0067] 本発明のデータクリーニング処理プログラムでは、データ処理装置に格納されるデータクリーニング処理プログラムにおいて、前記データ処理装置は、データ記録媒体と、当該データ記録媒体へのアクセス制御を行う制御手段とを備えており、前記データ記録媒体は、データ領域とFAT領域とに区分して前記制御手段で管理されており、前記データ領域は、ファイルデータを記録する複数のクラスタを有し、且つ、前記フ

ァイルデータを1又は2以上のクラスタに分散して記録しており、前記FAT領域は、前記クラスタを特定するアドレスが付された複数の記録領域を有し、且つ、各記録領域に対応するクラスタに記録されたファイルデータに連続するデータが記録されたチェーンクラスタのアドレス又は開放符号のいずれかを各記録領域毎に記録しており、前記FAT領域を参照して、開放符号が記録された全ての記録領域のアドレスを抽出し、抽出したアドレスに対応するクラスタに任意のダミーデータを上書きするようにした。

本発明を実施すると、データ記録媒体に記録されたデータを削除操作したり、更新操作をして最新データを作成した際に、データ領域のクラスタに残存する管理不要なデータを、任意のダミーデータで上書きすることができ、確実に消去することができる。

[0068] 本発明のデータクリーニング処理プログラムでは、データ処理装置に格納されるデータクリーニング処理プログラムにおいて、前記データ処理装置は、データ記録媒体と、当該データ記録媒体へのアクセス制御を行う制御手段とを備えており、前記データ記録媒体は、データ領域とFAT領域とに区分して前記制御手段で管理されており、前記データ領域は、ファイルデータを記録する複数のクラスタを有し、且つ、前記ファイルデータを1又は2以上のクラスタに分散して記録しており、前記FAT領域は、前記クラスタを特定するアドレスが付された複数の記録領域を有し、且つ、各記録領域に対応するクラスタに記録されたファイルデータに連続するデータが記録されたチェーンクラスタのアドレス又は開放符号のいずれかを各記録領域毎に記録しており、前記データ領域には特定ソフトウェアが格納されており、前記特定ソフトウェアは、データ領域の一部をソフトウェア管理領域として確保すると共に、作成したファイルデータの保存時には、最新の更新ファイルデータを旧データと区分して前記データ領域に記録し、更に、当該ファイルに係る最新の更新データ及び全ての旧データを記録したクラスタを示すFATデータを前記ソフトウェア管理領域に記録する構成とされ、前記特定ソフトウェアで作成したファイルデータを指定し、前記ソフトウェア管理領域に記録されたFATデータを参照して当該ファイルに係るデータの記録された全てのクラスタアドレスを抽出すると共に、前記FAT領域を参照して開放符号が記録された全ての記録領域のアドレスを抽出し、抽出した双方のアドレスの論理積アドレスに対応

するクラスタに任意のダミーデータを上書きするようにした。

本発明を実施すると、制御手段で管理されているファイルデータが記録されているクラスタを除くクラスタにのみ任意のダミーデータが上書きされるので、指定したファイルのデータクリーニング処理を短時間に完了することができる。

[0069] 前記第二の目的を達成するために提案される本発明は、データ記録媒体と、オペレーティングシステムによってデータ記録媒体へのアクセス制御を行う制御手段とを備えたデータ処理装置に格納されるデータクリーニング処理プログラムであって、前記データクリーニング処理プログラムはオペレーティングシステム上で動作すると共に、これらのプログラム及びシステムはデータ記録媒体に格納され、前記データ記録媒体に格納されたファイルを指定すると、指定したファイルに応じて、制御手段によって、クリーニング処理に必要なオペレーティングシステムの一部のファイル又はデータクリーニング処理プログラム自身又はこれらの双方をメインメモリに退避し、データ記録媒体又はメインメモリのオペレーティングシステムを参照しつつデータ記録媒体又はメインメモリのデータクリーニング処理プログラムに従って、指定したファイルが格納されていたデータ記録媒体の該当する記録領域に順次所定データを上書きする上書き処理を行うと共に、指定したファイルにオペレーティングシステムが含まれないときは、上書き処理したファイルをオペレーティングシステムの管理から削除させる処理を行うデータクリーニング処理プログラムである。

[0070] ここで、本発明のデータクリーニング処理プログラムはオペレーティングシステム(OS)上で動作するプログラムであり、データクリーニング処理プログラム及びOSはいずれもデータ記録媒体に格納(記録)されている。従って、データクリーニング処理プログラムが、OSやデータクリーニング処理プログラム自身を上書き(クリーニング処理)すると、上書き処理の途中でデータ処理装置はフリーズしてしまう。

[0071] しかし、本発明を実施すると、クリーニング処理に必要なOSの一部のファイル、又は、データクリーニング処理プログラム自身、又は、これらの双方をメインメモリに退避(コピー)することができる。従って、クリーニング処理をメインメモリに退避したOSやデータクリーニング処理プログラムから行うことができるので、データ記録媒体に記録されたOSやデータクリーニング処理プログラムが消去されても、データ処理装置をフ

リーズさせずに済む。

[0072] 本発明では、データ記録媒体に記録されたOSを構成するファイルのみをクリーニング処理する場合においても、クリーニング処理に必要なOSの一部のファイルをメインメモリに退避し、データ記録媒体に記録されたデータクリーニング処理プログラムが、メインメモリに退避したOSを参照してデータ記録媒体に記録されたOSをクリーニング処理することができる。

[0073] また、本発明では、データクリーニング処理プログラム自身をクリーニング処理する場合には、データクリーニング処理プログラムをメインメモリに退避し、メインメモリに退避したデータクリーニング処理プログラムが、データ記録媒体に記録されたOSを参照してデータ記録媒体に記録されたデータクリーニング処理プログラムをクリーニング処理することができる。

[0074] さらに、OSとデータクリーニング処理プログラムをメインメモリに退避し、データ記録媒体に記録された全てのファイルをクリーニング処理することもできる。クリーニング処理の対象から外すことにより、OSや、データクリーニング処理プログラム、他のソフトウェアやデータ類を任意にデータ記録媒体に残すこともできる。

[0075] すなわち、本発明によれば、ハードディスクに格納されたファイルのうち、上書き消去しようとするファイルを任意に指定することにより、指定したファイルにOSやデータクリーニング処理プログラムが含まれる場合であっても、フリーズすることなく上書き処理を実行することができる。

これにより、不要なファイルを上書き消去して必要なファイルだけをハードディスクに格納した状態を容易に作り出すことができ、しかも、上書き消去したファイルの元データを読み取られることもない。

[0076] また、本発明によれば、指定したファイルにOSが含まれないとき、すなわち、OSを上書き消去しない場合は、データクリーニング処理プログラムによって上書き処理したファイルを、OSの管理から削除させる処理を行う。これにより、データ記録媒体に格納されているファイルをOSで管理することが可能となる。

[0077] 本発明を実施する場合に、予めメインメモリの一部にRAMディスクを形成しておき、このRAMディスクにOSやデータクリーニング処理プログラムを退避させることもで

きる。

この構成によれば、データ処理装置が、RAMディスクに退避したOSやデータクリーニング処理プログラムを実行し、データ記録媒体に格納されたOSやデータクリーニング処理プログラムを上書き消去しても、データ処理装置はフリーズすることなく上書き消去処理(データクリーニング処理)を継続することができる。

[0078] また、RAMディスクは、ハードディスク等のメカニカルな記録媒体よりも高速なアクセスが可能であり、データ処理装置はクリーニング処理を高速に実行することができる。更に、データ処理装置の通電を遮断する、又はリセットすると、RAMディスクに退避させたOSやデータクリーニング処理プログラムは消去される。従って、再起動させたデータ処理装置のメインメモリには残存するファイルはなく、メモリエリアを圧迫することもない。

[0079] 本発明のデータクリーニング処理プログラムは、前述の構成に加えて、前記データ記録媒体に格納された全てのファイルを指定可能であり、当該全てのファイルを指定すると、制御手段によって、クリーニング処理に必要なオペレーティングシステムの一部のファイルとデータクリーニング処理プログラム自身とをメインメモリに退避し、メインメモリに退避したオペレーティングシステムを参照しつつ、メインメモリに退避したデータクリーニング処理プログラムに従って前記上書き処理を行う構成とすることが好ましい。

[0080] 前記したように、削除指定したファイルにOSやデータクリーニング処理プログラムが含まれる場合、データ記録媒体に格納されたデータクリーニング処理プログラムに従って、データ記録媒体に格納されている全てのファイルを順に上書き消去すると、OSやデータクリーニング処理プログラム自身の上書き消去の途中に処理がフリーズする。

[0081] しかし、本発明では、データ記録媒体に格納された全てのファイルを指定すると、クリーニング処理に必要なOSの一部のファイルとデータクリーニング処理プログラム自身とをメインメモリに退避する。そして、退避したデータクリーニング処理プログラムが、同じく退避したOSを参照し、データ処理装置をフリーズさせることなくデータ記録媒体上の全てのファイルに上書き処理を行う。

[0082] また、本発明を実施してデータ記録媒体に格納された全てのファイルを上書き消去すると、データ記録媒体上に記録されていたファイルの元データの復元を完全に阻止することができ、元データを読み取られる恐れがなくなる。

また、データ記録媒体に格納されていた全てのファイルを上書き消去するので、OSを再インストールすることにより、データ記録媒体を初期状態に復元することが可能である。

すなわち、本発明によれば、データ記録媒体の全てのファイルを容易に上書き消去することができるデータクリーニング処理プログラムを提供できる。

[0083] 本発明のデータクリーニング処理プログラムは、前述の構成に加えて、前記制御手段が、オペレーティングシステムを構成するファイルのプロテクトを解除可能な構成とすることもできる。

[0084] データ記録媒体に格納されるOSは、OSを構成するファイルの誤消去を防止するために、インストール時に各ファイルにプロテクトが施されることがある。このため、データクリーニング処理プログラムによる上書き消去が阻止されることとなり、データ記録媒体に格納された全てのファイルを上書き消去することができない。

[0085] 本発明によれば、データクリーニング処理プログラムにより、制御手段は、OSを構成するファイルに施されたプロテクトを解除することができる。これにより、データ記録媒体に格納されたOSを構成する全てのファイルを上書き消去することが可能となる。

[0086] 本発明のデータクリーニング処理プログラムは、前記データ記録媒体に格納されたファイルのうち、前記オペレーティングシステムを除き、データクリーニング処理プログラム又は当該データクリーニング処理プログラムと他のソフトウェア又はデータの少なくともいずれかのファイルを指定可能であり、当該ファイルを指定すると、制御手段によって、データクリーニング処理プログラム自身をメインメモリに退避し、データ記録媒体に格納されたオペレーティングシステムを参照しつつ、メインメモリに退避したデータクリーニング処理プログラムに従って前記上書き処理を行う構成とすることが好ましい。

[0087] 前記したように、指定したファイルにデータクリーニング処理プログラム自身が含まれる場合、データ記録媒体に格納されたデータクリーニング処理プログラムに従って

自らを上書き消去すると、上書き消去の途中に処理がフリーズする。

[0088] しかし、本発明によれば、データクリーニング処理プログラムに関連するファイルを指定すると、データクリーニング処理プログラム自身をメインメモリに退避し、データ記録媒体に格納されたOSを参照しつつ、メインメモリに退避したデータクリーニング処理プログラムに従ってデータ記録媒体上のファイルを上書き処理する。これにより、データ記録媒体に格納されたデータクリーニング処理プログラムが上書き消去されても、メインメモリに退避したデータクリーニング処理プログラムによって上書き処理を継続させることが可能であり、データ処理装置がフリーズすることがない。

すなわち、本発明によれば、OSを再インストールすることなく、データ記録媒体をOSだけが格納された初期状態に容易に復元することができるデータクリーニング処理プログラムを提供することができる。

[0089] また、本発明では、データクリーニング処理プログラムによって上書き処理したファイルを、OSの管理から削除させる処理を行う。これにより、データ記録媒体に格納されるファイルをOSで管理することが可能となる。

[0090] また、本発明によれば、OSを除き、データクリーニング処理プログラムを含む他のソフトウェア及びデータの全てのファイルを指定してデータクリーニング処理を行うと、データ記録媒体にはOSだけが格納された状態となる。更に、上書き消去されたデータクリーニング処理プログラムや他のソフトウェア及びデータ類の元データを読み取られることがない。

これにより、データ記録媒体をOSだけが格納された初期状態に復元することができ、しかも、OSを再インストールする手間も不要となる。

[0091] 本発明のデータクリーニング処理プログラムは、前記データ記録媒体に格納されたファイルのうち、前記オペレーティングシステムとデータクリーニング処理プログラムとを除き、他のソフトウェア又はデータの少なくともいずれかのファイルを指定可能であり、当該ファイルを指定すると、制御手段によって、データ記録媒体に格納されたオペレーティングシステムを参照しつつ、データ記録媒体に格納されたデータクリーニング処理プログラムに従って前記上書き処理を行う構成とすることが好ましい。

[0092] 本発明によれば、OSやデータクリーニング処理プログラムが上書き処理指定され

ないので、OSやデータクリーニング処理プログラム自身が上書き消去されない。従って、OSやデータクリーニング処理プログラム自身をメインメモリに退避することなく、データ記録媒体に格納されたOSを参照しつつデータ記録媒体に格納されたデータクリーニング処理プログラムに従って上書き処理を行うことができる。これにより、指定した他のソフトウェア又はデータ類を上書き消去することができ、これらの元データが読み取られることもない。

[0093] また、データクリーニング処理プログラムによって上書き処理したファイルを、OSの管理から削除させる処理を行う。これにより、データ記録媒体に格納されているファイルをOSで管理することが可能となる。

[0094] ここで、データ記録媒体に格納されたファイルをOSによって削除すると、OSが管理するディレクトリ領域及びFAT(File Allocation Table) 領域に記録されていた当該ファイルに係るデータが削除されるだけで、当該ファイルの実データ(データ本体)はデータ記録領域に残存したままとなる。このため、OSによるファイルの削除を継続すると、実データが記録されていたデータ記録領域に別のデータが上書きされるまでは、削除されたファイルの実データが残存することとなる。

[0095] しかし、本発明によれば、データクリーニング処理プログラムによって、指定したファイルをOSの管理から削除すると共に、当該ファイルの実データを上書き消去する。すなわち、ファイルを指定してデータクリーニング処理を行うと、その都度、実データが上書き消去されるので、OSによって削除を行う場合のように、削除したファイルの実データが残存することがない。

[0096] また、日常のソフトウェアやデータの削除を本発明のデータクリーニング処理によって行えば、過去に削除したファイルの実データが残存しない。

従って、他のソフトウェア及びデータの全てのファイルを指定してデータクリーニング処理を行うことにより、データ記録媒体を、OSとデータクリーニング処理プログラムだけが格納された状態に復元することができる。

すなわち、データクリーニング処理によってデータ記録媒体を、OSとデータクリーニング処理プログラムだけが格納された初期状態に容易に復元することができ、しかも、OSを再インストールする手間も不要である。

すなわち、本発明によれば、OS及びデータクリーニング処理プログラム自身を再インストールすることなく、データ記録媒体をOSとデータクリーニング処理プログラムとが格納された状態に容易に復元することができるデータクリーニング処理プログラムを提供することができる。

[0097] 本発明のデータクリーニング処理プログラムは、前述の構成に加えて、前記データ記録媒体は、オペレーティングシステム又はBIOSで管理される隠し領域を備え、当該隠し領域はオペレーティングシステムのインストール機能を備えると共に、前記データクリーニング処理プログラムによる上書き処理が禁止される構成とされている。

[0098] 本発明によれば、データクリーニング処理によって、隠し領域の上書き処理が行われないので、隠し領域に格納されたOSのインストールに要するファイルが消去されることがない。

[0099] 従って、前記データ記録媒体が、オペレーティングシステム又はBIOSで管理される隠し領域を備え、当該隠し領域がオペレーティングシステムのインストール機能を備えると共に、メインメモリに退避させたデータクリーニング処理プログラム及びオペレーティングシステムの一部のファイルによって、上書き処理が禁止されるように構成してもよい。そして、データ記録媒体に格納された全てのファイルを上書き消去した後に、隠し領域のインストール機能によってデータ記録媒体のデータ記録領域にOSを再インストールすることができる。

これにより、データ記録媒体にOSだけが格納された初期状態に復元することができる。よって、第三者に元データが復元されて読み取られる恐れがない。また、隠し領域がOSのインストール機能を備えるので、別のOSインストールディスクなどを添付する必要がなく、省コスト化が図られると共に、OSインストールディスクを保管管理する手間が不要である。

[0100] 本発明において、隠し領域をOSで管理する構成を採ることができる。すなわち、当該隠し領域内に格納したOS、又は、別のドライブのOSを用いてインストール機能を起動させる構成を採ることができる。

また、本発明において、隠し領域をBIOSで管理する構成とすることも可能である。すなわち、データ記録媒体にOSが格納されていない場合は、BIOSによってインスト

ール機能を起動させる構成を採ることができる。

[0101] ところで、データ記録媒体に格納されたOSを構成する多数のファイルは、単体で安定して動作するファイルもあれば、OSには含まれないデバイスドライバなどと連携して動作するファイルもある。

このため、前述の本発明のように、データ記録媒体にOSを残した状態でデータクリーニング処理を行うと、OSに含まれないデバイスドライバなどが全て消去されることとなり、OSの動作が不安定になることがある。

[0102] しかし、本発明によれば、隠し領域にオペレーティングシステムのインストールに必要なファイルが格納されている。従って、前述の本発明によってデータクリーニング処理を行った結果、仮にOSの動作が不安定になったような場合でも、制御手段によってメインメモリにデータクリーニング処理プログラムとオペレーティングシステムの一部のファイルを退避させ、退避したデータクリーニング処理プログラムとオペレーティングシステムの一部のファイルによってデータクリーニング処理を行い、OSを含む全ファイルを消去した後に、隠し領域のインストールに必要なファイルによってOSを再インストールすることができる。これにより、データ記録媒体をOSのみが格納された状態に復元することができ、しかも、データ処理装置の安定した動作を確保することが可能となる。

すなわち、本発明によれば、前記発明に適用することにより、隠し領域のインストール機能を利用してOSを容易にインストールすることができ、データ記録媒体を容易に初期状態に復元することが可能となる。

[0103] 本発明のデータクリーニング処理プログラムでは、前述の構成に加えて、前記上書き処理が、同一データ又は異なるデータを、任意の所定回数だけ繰り返し上書きするように構成することもできる。

[0104] ここで、ハードディスクなどの磁気データ記録媒体では、媒体が磁化される磁極を所定の閾値で仕切ることによって「1」,「0」の判別を行うデータ記録方式が採用される。ところが、「1」が記録された部位に「0」を上書きすると、「0」の読み出しは行われるものの、磁極は完全には反転していない。そのため、磁化レベルを詳細に解析する特殊処理を行うと、データを上書きしているにも拘わらず、上書き前の元データが読

み出される可能性が生じる。

[0105] しかし、本発明を実施すれば、データ記録領域に同一データ又は異なるデータを繰り返して上書き処理するので、磁化の履歴をたどって元データを復元することが極めて困難になる。その結果、元データが読み取られることを効果的に阻止することが可能となる。

[0106] 上書きするデータは、例えば、「00H」や「FFH」あるいは「E5H」などの任意のデータを採用することができ、いずれか一つのデータ、又はこれらの複数のデータを所定回数だけ繰り返して上書きすることにより、元データの読み取りを完全に阻止することが可能となる。

すなわち、本発明によれば、元データが読み取られることを完全に阻止することができ、セキュリティを向上したデータクリーニング処理プログラムを提供できる。

[0107] 本発明のデータクリーニング処理プログラムにおいては、前述の構成に加えて、前記データ記録媒体としてハードディスクを選定するのが好ましい。

[0108] ハードディスクは、他のデータ記録媒体に比べて記録容量が著しく大きく、通常、OSを格納したブート用の記録媒体として使用されている。本発明によれば、データクリーニング処理プログラムを用いてデータ記録媒体であるハードディスクに記録された元データを容易に上書き消去することができ、元データの読み取りを完全に阻止してセキュリティを確保することが可能となる。

すなわち、本発明によれば、ハードディスクに記録された元データが読み取られることを完全に阻止することができ、セキュリティを向上したデータクリーニング処理プログラムを提供できる。

[0109] 本発明のデータクリーニング処理プログラムでは、データ処理装置に格納されるデータクリーニング処理プログラムにおいて、前記データ処理装置は、データ記録媒体と、オペレーティングシステムによって当該データ記録媒体へのアクセス制御を行う制御手段とを備えており、前記データクリーニング処理プログラムはオペレーティングシステム上で動作すると共に、これらのプログラム及びシステムはデータ記録媒体に格納されており、前記データ記録媒体に格納されたファイルをクリーニング処理指定する際に、前記データ処理装置がデータクリーニング処理の途中で停止しないように

、データクリーニング処理に必要なオペレーティングシステムの一部のファイル又はデータクリーニング処理プログラム又はこれらの両方をメインメモリに退避させ、メインメモリに退避したデータクリーニング処理に必要なオペレーティングシステムの一部のファイル又はデータクリーニング処理プログラムによってデータクリーニング処理を行うようにした。

本発明では、メインメモリに退避したデータクリーニング処理に必要なオペレーティングシステムの一部のファイル又はデータクリーニング処理プログラムによってデータクリーニング処理を行うようにしたので、データ処理装置をデータクリーニング処理の途中で停止させることなく、クリーニング処理を完了することができる。

発明の効果

[0110] 第一の目的を達成する本発明によれば、データ記録媒体に残存する不要データを読み取り不能にすることができる。従って、データを復元されて漏洩することを防止することができ、データ漏洩のセキュリティを確保することのできるデータクリーニング処理プログラムを提供することができる。

[0111] 第二の目的を達成する本発明によれば、データ記録媒体に格納されたOSやデータクリーニング処理プログラム自身を含む指定ファイルを容易に上書き消去することができ、データ記録媒体のファイルの格納を、容易に所望する状態にすることのできるデータクリーニング処理プログラムを提供することができる。

図面の簡単な説明

[0112] [図1](a)ー(d)は、本発明の実施形態に係るデータクリーニング処理プログラムの処理を模式的に示す説明図である。

[図2]本発明の別の実施形態に係るデータクリーニング処理プログラムによって、保存又は削除されたファイルを処理する過程を模式的に示す説明図である。

[図3]図2のデータクリーニング処理プログラムによって、更新又は更新後に削除されたファイルを処理する過程を模式的に示す説明図である。

[図4]本発明の実施形態に係るデータクリーニング処理プログラムを格納したデータ処理装置の内部構成を示す模式図である。

[図5]図4のデータ処理装置においてデータ記録媒体に格納された全てのファイルを

指定してデータクリーニング処理を行う課程を示す模式図である。

[図6]図5のデータクリーニング処理が完了した状態を示す模式図である。

[図7]図6のデータクリーニング処理の施されたデータ記録媒体にOSを再インストールした状態を示す模式図である。

[図8]図4のデータ処理装置において、OSを除く他の全てのファイルを指定してデータクリーニング処理を行う課程を示す模式図である。

[図9]図8のデータクリーニング処理が完了した状態を示す模式図である。

[図10]図4のデータ処理装置において、OS及びデータクリーニング処理プログラムを除く他の全てのファイルを指定してデータクリーニング処理を行う課程を示す模式図である。

[図11]図10のデータクリーニング処理が完了した状態を示す模式図である。

[図12]特許文献1に開示されたハードディスクの記録領域の管理構成を模式的に示す説明図である。

[図13](a)ー(f)は、図12に示すハードディスクにファイルデータが記録される過程を模式的に示す説明図である。

[図14](a)ー(f)は、図12に示すハードディスクに記録されたファイルデータが削除される過程を模式的に示す説明図である。

[図15](a),(b)は、特定ソフトウェアによって図12に示すハードディスクにファイルデータが記録される処理を模式的に示す説明図である。

発明を実施するための最良の形態

[0113] 以下に、図面を参照して本発明の実施形態を説明する。

図1は、本発明の実施形態に係るデータクリーニング処理プログラムで実行する処理を模式的に示す説明図である。

[0114] なお、ここでは制御手段とは、OSと当該OSによってデータ記録媒体へのアクセス制御を実行する中央処理装置(CPU)とを含んだ構成を指す。また、本実施形態では、データ記録媒体としてハードディスクを採用しており、当該ハードディスクへのアクセス制御を制御手段で行うものとして述べる。

[0115] また、以下の説明では、FAT14を形成する各記録領域14aに付されるアドレスと、

データ領域17の各クラスタに付されるアドレスには、いずれも「00H」から始まる16進2バイトで示される値を採用している。「00H」(値)は開放符号を示しており、「FFH」(値)はデータ終端符号を示している。

[0116] 本実施形態において、データクリーニング処理を行うにあたり、データクリーニング処理プログラムを予めハードディスクにインストールしておく。このデータクリーニング処理プログラムは、制御手段によって実行される。

[0117] 図1(a)ー(c)は、ハードディスク10に3つのファイル「ABC」、「DEF」、「XYZ」が記録された状態を示している。ファイル「ABC」は、図1(b)のように、エントリアドレスが00H、ファイルサイズが6KB(キロバイト)のテキストファイル(TXT)である。すなわち、ファイル「ABC」は、図1(a),(c)に示されるように、アドレスが01H, 02H, 03H, 14H, 15H, 22Hの6つのクラスタ17aにファイルデータが分散して記録されている。

[0118] ファイル「DEF」は、図1(b)に示すように、エントリアドレスが05H、ファイルサイズが5KB(キロバイト)のドキュメントファイル(DOC)である。すなわち、ファイル「DEF」は、図1(a),(c)に示されるように、アドレスが05H, 08H, 09H, 18H, 27Hの5つのクラスタ17aにファイルデータが分散して記録されている。

[0119] 又、ファイル「XYZ」は、図1(b)に示すように、エントリアドレスが0CH、ファイルサイズが4(KB)のドキュメントファイル(DOC)である。すなわち、ファイル「XYZ」は、図1(a),(c)で示されるように、アドレスが0CH, 1BH, 1EH, 2DHの4つのクラスタ17aにファイルデータが分散して記録されている。

[0120] すなわち、図1は、「ABC」、「DEF」、「XYZ」の3つのファイルが、ハードディスク10内に存在し、且つ、OSで管理されている状態を示している。

ところで、ハードディスク10に記録されるファイルデータが、図1(a)ー(c)に示す状態に至るまでには、前記3つのファイル以外の別のファイルが保存され、且つ、削除されている。これら削除された別ファイルが記録されていたFAT14の記録領域14aには開放符号「00H」が上書きされている。さらに、この削除された別ファイルに対応するディレクトリ領域16の情報は削除されている。

[0121] しかし、前記したように、データ領域17の対応するクラスタ17aには、削除された別ファイルに係る実データが依然として残存する。削除された別ファイルに係る実デー

タが記録されたクラスタ17aは、図1(c)において斜線で示されている。前記3つのファイルの実データが、削除された別ファイルの実データが記録されたクラスタ17aに上書き保存される。その結果、別ファイルの実データは、図1(c)に示すようにデータ領域17に散在してしまう。

[0122] 本実施形態のデータクリーニング処理プログラムは、制御手段によって起動され、クリーニング処理が開始される。

データクリーニング処理プログラムに従って制御手段は、まず、FAT領域13のFAT14を参照して開放符号「00H」が記録された全ての記録領域14aのアドレスを抽出する。すなわち、図1(a)において、開放符号「00H」が記録されている全ての記録領域14aのアドレス04H, 06H, 07H, 0AH等を抽出する。この抽出された記録領域14aのアドレスは、データ領域17のクラスタ17aのうち、一度もデータが記録されていないクラスタ17aか、又は、不要なデータ(削除操作済みのデータ)が残存するクラスタ17aのアドレスと対応している。

[0123] 次いで、制御手段は、抽出した記録領域14aのアドレスに対応するデータ領域17のクラスタ17aに、所定データ(任意のダミーデータ)である「00H」(値)を順次上書き保存する。すなわち、図1(c)に示すように、アドレス04H, 06H, 07H, 0AH等のクラスタ17aに順次「00H」(値)を上書きする。そして制御手段は、抽出した全ての記録領域14aのアドレスに対応するデータ領域17のクラスタ17aを上書きすると、データクリーニング処理を終了する。

[0124] 以上の処理により、OSで管理される3つのファイル「ABC」、「DEF」、「XYZ」以外の、過去に削除処理が行われた別ファイルに係るデータや、更新処理が行われたファイルの全ての旧データに係るデータが、読み取り不能となる。従って、特殊な解析ソフトウェアによってデータ領域17に残存する削除操作済みのデータが復活(復元)されることを阻止することができる。よって、復元されたデータが漏洩することを防止することができ、データのセキュリティを確保することが可能となる。

[0125] なお、本実施形態では、データ領域17のクラスタ17aへ上書きする所定データ(任意のダミーデータ)を「00H」としたが、上書きする所定データ(任意のダミーデータ)は、「FFH」や「E5H」などの任意のデータを選定することができる。また、これら複数

の所定データを、抽出したクラスタ17aに順次上書きすることにより、残存する不要データ(削除操作済みデータ)の読み取りをより完全に阻止することが可能となる。

[0126] また、本実施形態では、制御手段でデータクリーニング処理プログラムを起動することによってデータクリーニング処理を開始する構成としたが、例えば、データ処理装置のタイマ設定で、データクリーニング処理を開始する時刻を予め設定しておき、当該設定時刻に至ったときに自動的にデータクリーニング処理を開始させるようにしてもよい。また、他の処理(ワードプロセッサによる文章入力作業等)が所定時間継続して行われない場合に、自動的にデータクリーニング処理を開始させるようにしてもよい。

[0127] 次に、本発明の別の実施形態に係るデータクリーニング処理プログラムを説明する。

図2及び図3は、本実施形態に係るハードディスク10の記録領域を模式的に示す説明図である。図2及び図3に示すハードディスク10の構成は、前述の図12に示した構成と同じである。従って、図2及び図3におけるハードディスク10の構成には、図12に示すハードディスク10の構成と同一の符号を付しており、ここでは重複した説明を省略する。

[0128] 本実施形態のデータクリーニング処理プログラムは、特定ソフトウェア18によって作成されるファイルデータを選択的にデータクリーニング処理するものである。

なお、以下の説明では、データ記録媒体をハードディスクとして述べる。

[0129] 図2に示すように、特定ソフトウェア18をハードディスク10にインストールすると、特定ソフトウェア18は、OSの管理下においてデータ領域17の一部をソフトウェア管理領域19として確保する。OSは、ソフトウェア管理領域19に記録されるデータを削除することはできない。そして、特定ソフトウェア18は、OSで管理されるFAT領域13及びディレクトリ領域16とは別に、特定ソフトウェア18に係る各ファイルのデータが記録されたクラスタ17aを示すFATデータを、ソフトウェア管理領域19に記録する機能を備えている。

[0130] すなわち、特定ソフトウェア18で作成したファイル「No. 1」の保存処理を実行すると、図2に示すように、OSによって「No. 1」ファイルデータ30がデータ領域17のクラ

スタ17aに記録されてFAT管理が行われ、且つ、「No. 1」ファイルデータ30の記録されたクラスタアドレスを示すFATデータ30aをソフトウェア管理領域19に記録する。

[0131] FATデータ30aは、ファイル名とファイルデータアドレス及びファイル属性を関連付けたチェーンクラスタで構成される。すなわち、図2に示すファイル「No. 1」は、データ領域17のアドレス01H, 02H, 14H, 15H, 22Hの5つのクラスタ17aに、データが記録されていることを示している。

特定ソフトウェア18で作成した別のファイル「No. 2」の保存処理を実行した場合も、同様に、OSで管理が行われると共に、特定ソフトウェア18によってソフトウェア管理領域19にFATデータ35aが記録される。

[0132] 更に、特定ソフトウェア18で作成し保存されているファイル「No. 1」の更新保存処理を行うと、図3に示すように、ファイル「No. 1」の更新データ30と、更新前の旧データ31とが、データ領域17のクラスタ17aに別々に記録される。更に、更新データ30及び旧データ31の各々のFATデータ30a, 31aがソフトウェア管理領域19に記録される。

[0133] 制御手段が、更新保存処理を繰り返すと、ファイル「No. 1」に係る全てのデータ(更新データ30、旧データ31及び旧々データ32)がデータ領域17に区分して記録される。特定ソフトウェア18は、当該ファイル「No. 1」に係る全てのFATデータ30a, 31a, 32aをソフトウェア管理領域19に記録する機能を有する。

[0134] ここで、図3に示すように、ファイル「No. 1」の更新保存処理が行われた場合には、OSは、更新データ30のみを管理し、他の全ての旧データ31, 旧々データ32の記録されたクラスタ17aに対応するFAT14の記録領域14a(図1)を開放する。

[0135] このような処理機能を有する特定ソフトウェア18で作成したファイルがデータクリーニング処理される過程を、図2及び図3を参照して説明する。

[0136] まず、図2を参照して、特定ソフトウェア18で作成した「No. 1」ファイルデータ30の保存処理が行われた後に、データクリーニング処理を実行した場合を説明する。

データクリーニング処理プログラム20を起動すると、データ処理装置のディスプレイ(図示せず)上にファイル名の入力を促す画面が表示される。ここで、ファイル名としてファイル「No. 1」を入力する。

ファイル名を入力すると、制御手段は、ソフトウェア管理領域19に記録されたFATデータを参照して、ファイル「No. 1」に係る全てのFATデータ30aを読み出す。図2の場合は、ファイル「No. 1」に係るFATデータは30aのみである。そして、FATデータ30aに記録されたファイル「No. 1」に係る全てのチェーンクラスタアドレス(01H, 02H, 14H, 15H, 22Hの5つのクラスタ17aのアドレス)を抽出する。

[0137] 次いで、制御手段は、OSの管理するFAT14(図12参照)を参照して、開放符号「00H」の記録された記録領域14aのアドレスを全て抽出する。そして、制御手段は、前記FATデータ30aを参照して抽出したアドレスとFAT14を参照して抽出したアドレスとの論理積アドレスを演算する。ところが、ファイル「No. 1」は保存されたばかりでOSの管理下にある。このため、前記FATデータ30aを参照して抽出したアドレスは、いずれもFAT14を参照して抽出したアドレスと一致しない。

従って、FATデータ30aで示されるいずれのアドレスのクラスタ17aも上書きされることなくクリーニング処理を終了する。

[0138] すなわち、特定ソフトウェア18で作成し保存されたファイルに対してデータクリーニング処理を実行しても、データが上書きされることはない。

[0139] 一方、図2において、特定ソフトウェア18で作成され、且つ、保存された「No. 1」ファイルデータ30が削除され、その後にデータクリーニング処理を実行した場合には、上記とは処理が異なる。

すなわち、ファイル「No. 1」の削除処理を行うと、当該ファイル「No. 1」に係る「No. 1」ファイルデータ30が記録されたクラスタ17aに対応するアドレスのFAT14の記録領域14aに開放符号「00H」が上書きされて、当該クラスタ17aはOSの管理から開放される。

[0140] 「No. 1」ファイルデータ30が削除された後にデータクリーニング処理を実行すると、前記FATデータ30aを参照して抽出したアドレスの全てが、FAT14を参照して抽出したアドレスと一致する。従って、両者の論理積アドレスを演算することによって得られるアドレス01H, 02H, 14H, 15H, 22Hの5つのクラスタに所定データである「00H」(値)が上書きされる。更に、ソフトウェア管理領域19に記録されたFATデータ30aのファイル名及びチェーンクラスタアドレスにも「00H」(値)が上書きされる。

[0141] すなわち、特定ソフトウェア18で作成され、且つ、保存されたファイルが削除された後は、データクリーニング処理を実行することによって、当該「No. 1」ファイルデータ30及びFATデータの双方が上書き処理されて「No. 1」ファイルデータ30の読み取りが不能となる。

[0142] 次に、図3を参照して、特定ソフトウェア18で作成した「No. 1」ファイルデータ30の更新処理が行われた後に、データクリーニング処理を実行した場合について説明する。

データクリーニング処理プログラム20を起動すると、データ処理装置のディスプレイ(図示せず)上にファイル名の入力を促す画面が表示される。ここで、ファイル名としてファイル「No. 1」を入力する。ファイル名を入力すると、制御手段は、ソフトウェア管理領域19に記録されたFATデータを参照して、ファイル「No. 1」に係る全てのFATデータ30a, 31a, 32aを読み出す。

[0143] この場合は、図3に示すように、ファイル「No. 1」に係るFATデータは、更新データ30(最新データ)、旧データ31及び旧々データ32に対応するFATデータ30a, 31a及び32aである。そして制御手段は、各FATデータに記録されたファイル「No. 1」に係る全てのチェーンクラスタアドレスを抽出する。この場合、FATデータ30aからはアドレス01H, 02H, 14H, 15H, 22Hの5つのアドレスが抽出され、FATデータ31aからはアドレス25H, 26H, 2AH, 2BHの4つのアドレスが抽出される。さらに、FATデータ32aからはアドレス31H, 35H, 37H, 38Hの4つのアドレスが抽出される。

[0144] 次いで、制御手段は、OSの管理するFAT14(図12参照)を参照して、開放符号「00H」の記録された記録領域14aのアドレスを全て抽出する。そして、前記FATデータ30aを参照して、抽出したアドレスとFAT14とを参照し、これらの論理積アドレスを演算する。

[0145] ここで、ファイル「No. 1」は更新処理されており、OSは、更新データ30(最新データ)の記録されたクラスタアドレスだけをFAT14で管理し、旧データ31及び旧々データ32の記録されたクラスタアドレスに対応するFAT14は開放している。

[0146] 従って、「No. 1」ファイルデータ30が更新された後にデータクリーニング処理を実行すると、更新データ30のFATデータ30aを除き、旧データ31及び旧々データ32

のFATデータ31a及び32aに記録されたアドレスが、FAT14を参照して抽出されたアドレスと一致する。従って、両者の論理積アドレスを演算することによって得られるアドレス25H, 26H, 2AH, 2BHの4つのクラスタ17aに記録されたデータと、アドレス31H, 35H, 37H, 38Hの4つのクラスタ17aに記録されたデータが、所定データである「00H」(値)で上書きされる。更に、ソフトウェア管理領域19に記録されたFATデータ31a, 32aのファイル名及びチェーンクラスタアドレスにも「00H」(値)が上書きされる。

[0147] すなわち、特定ソフトウェア18で作成されたファイルが更新保存された後に、データクリーニング処理を実行すると、当該ファイルの更新データ(最新データ)を除く全ての旧データに係るデータ及びFATデータの双方が上書き処理され、上書き処理されたデータの読み取りは不可能になる。

[0148] 次に、図3に示すように、特定ソフトウェア18で作成され、且つ、更新保存された「No. 1」ファイルデータ30が削除され、その後に、データクリーニング処理を実行した場合について説明する。

データクリーニング処理プログラム20を起動すると、データ処理装置のディスプレイ(図示せず)上にファイル名の入力を促す画面が表示される。ここで、ファイル名としてファイル「No. 1」を入力すると、制御手段は、ソフトウェア管理領域19に記録されたFATデータを参照して、ファイル「No. 1」に係る全てのFATデータ30a, 31a, 32aを読み出す。

[0149] この場合、削除されていない場合と同様に、図3に示すように、ファイル「No. 1」に係るFATデータは、更新データ30(最新データ)、旧データ31及び旧々データ32の各々のFATデータ30a, 31a及び32aである。制御手段は、これらのFATデータを全て読み出す。そして、制御手段は、各FATデータに記録されたファイル「No. 1」に係る全てのチェーンクラスタアドレスを抽出する。この場合、FATデータ30aからはアドレス01H, 02H, 14H, 15H, 22Hの5つのクラスタ17aのアドレスが抽出され、FATデータ31aからはアドレス25H, 26H, 2AH, 2BHの4つのクラスタ17aのアドレスが抽出される。さらに、FATデータ32aからはアドレス31H, 35H, 37H, 38Hの4つのクラスタ17aのアドレスが抽出される。

[0150] 次いで、制御手段は、OSの管理するFAT14(図12参照)を参照して、開放符号「00H」(値)の記録された記録領域14aのアドレスを全て抽出する。

そして、前記FATデータ30aを参照して抽出したアドレスと、FAT14を参照して抽出したアドレスの論理積アドレスを演算する。

[0151] ここで、ファイル「No. 1」は既に削除処理されており、OSは、ファイル「No. 1」に係る更新データ30(最新データ)、旧データ31及び旧々データ32の記録された全てのクラスタアドレスに対応するFAT14を開放している。

[0152] 従って、「No. 1」ファイルデータ30が削除された後にデータクリーニング処理を実行すると、更新データ30、旧データ31及び旧々データ32のFATデータ30a, 31a及び32aを参照して抽出した全てのアドレスが、FAT14を参照して抽出したアドレスと一致する。従って、両者の論理積アドレスを演算することによって得られるアドレス01H, 02H, 14H, 15H, 22Hの5つのクラスタ17aと、アドレス25H, 26H, 2AH, 2BHの4つのクラスタ17aと、アドレス31H, 35H, 37H, 38Hの4つのクラスタ17aに対して、所定データである「00H」が上書きされる。更に、ソフトウェア管理領域19に記録されたFATデータ30a, 31a及び32aのファイル名及びチェーンクラスタアドレスにも「00H」が上書きされる。

[0153] すなわち、特定ソフトウェア18で作成されたファイルが更新保存され削除された後に、データクリーニング処理を実行すると、当該ファイルに係る全てのデータ及びFATデータの双方が上書き処理されてデータの読み取りが不能となる。

[0154] このように、本実施形態のデータクリーニング処理プログラム20は、FATデータを独自にソフトウェア管理領域19に記録する特定ソフトウェア18を用いる場合にも、管理不要なデータを短時間に効率良く上書きして読み取り不能にすることができる。従って、データが復元されて漏洩することを阻止することができ、セキュリティを確保することが可能となる。

[0155] なお、本実施形態では、データクリーニング処理の開始に際して、特定ソフトウェア18で作成されたファイル名を指定して当該ファイルのみのクリーニング処理を行う構成とした。しかし、例えば、特定ソフトウェア18のファイルに付される拡張子を付してファイル名をワイルドカード指定することにより、当該特定ソフトウェア18で作成した全て

のファイルについてデータクリーニング処理を一斉に行うことも可能である。

[0156] 以上、本発明の実施形態を説明したが、図1に示したデータクリーニング処理プログラムと、図2及び図3に示したデータクリーニング処理プログラム20の機能を併せ持つ処理プログラムをデータ記録装置にインストールし、制御手段によっていずれか一方のプログラムを選択的に起動してデータクリーニングを行わせることも可能である。

[0157] また、前記実施形態では、データ記録媒体としてハードディスクを例に挙げて説明したが、本発明はこのような構成に限られるものではない。例えば、フレキシブルディスクやCD−RW、DVD−RAM、DVD−RW、MOなど、FAT領域とデータ領域とに区分して管理されるデータ記録媒体であれば、本発明のデータクリーニング処理プログラムを用いて不要データの復元を効果的に阻止することが可能である。

[0158] また、前記実施形態では、OSによってFAT領域13にFAT14が記録される構成として述べたが、FATに加えて、ファイル情報に係るディレクトリデータやデータの一部が格納されるOSを採用する場合であっても、本発明のデータクリーニング処理プログラム20によってデータクリーニング処理を行うことが可能である。

[0159] 以下では、図4ー図7を参照して本発明の第二の目的を達成するための実施形態について説明する。

図4は本発明の実施形態に係るデータクリーニング処理プログラムを格納したデータ処理装置の内部構成を示す模式図であり、図5は図4のデータ処理装置においてデータ記録媒体に格納された全てのファイルを指定してデータクリーニング処理を行う課程を示す模式図であり、図6は図5のデータクリーニング処理が完了した状態を示す模式図であり、図7は図6のデータクリーニング処理の施されたデータ記録媒体にOSを再インストールした状態を示す模式図である。

[0160] なお、以下の説明では、データ処理装置1に設けられるディスプレイやキーボードなどの周辺機器を省略している。又はハードディスク(データ記録媒体)10に格納されるOSをWindowsとして述べる。

[0161] 図4に示すように、本実施形態のデータ処理装置1は、中央処理装置(CPU)で成る制御手段2と、制御手段2によって直接データを読み書き可能なメインメモリ3と、ハードディスク(データ記録媒体)10と、不揮発性メモリに格納されたBIOS5とを備えて

構成される。ハードディスク10は、記録領域21を備えている。記録領域21は、インストールされたOS24で管理される記録領域22と、BIOS5で管理される隠し領域23とに分割されている。

[0162] OS24は、記録領域22を複数の領域に区分して管理する。すなわち、記録領域22は、OS24によって、MBR(Master Boot Record)領域11、BPB(BIOS Parameter Block)領域12、FAT(File Allocation Table)領域13、ディレクトリ領域16及びデータ領域17に区分して管理される。

従って、記録領域22は、OS24の格納された領域(24)とアプリケーションやデータが格納されるデータ領域17に区分されている。

[0163] MBR領域11は、OSの起動プログラム(OS Boot Loader)や、そのパーティション位置、サイズなどの位置情報であるパーティションテーブルが格納される領域である。BPB12は、周辺機器に対する入出力を管理するためのFATやディレクトリエントリに関するデータであるBIOSパラメータが格納される領域である。

[0164] FAT領域13は、FAT14とそのコピーであるFAT15とが格納される領域である。FAT14は、アドレスデータを記録可能な複数の記録領域で形成され、各記録領域にはデータ領域17のクラスタアドレスに対応させたアドレスが付されている。すなわち、FAT14の記録領域に記録されるアドレスは、ファイルデータが記録されるデータ領域17のチェーンクラスタアドレスを示している。

FAT15もFAT14と同一の記録領域で形成されている。FAT15は、FAT14のデータが破壊した場合のバックアップ動作を行う。

[0165] ディレクトリ領域16は、ファイル情報が格納される領域である。ディレクトリ領域16は、ハードディスク10に記録されるファイル毎に、ファイル名、ディレクトリ名、拡張子、作成日時、最終更新日時、ファイルサイズ、エントリアドレス、属性などのファイルに関する情報が格納される。

[0166] データ領域17は、複数のアプリケーション25, 26やデータ30, 31が格納される領域である。データ領域17は、データを記録する複数のクラスタを備えており、各クラスタにはアドレスが付されている。本実施形態では、データ領域17にデータクリーニング処理プログラム20が予めインストールされており、当該プログラム20はOS24上で

動作する。

[0167] また、隠し領域23は、BIOS5で管理される領域である。隠し領域23には、OS24をインストールするためのインストールプログラムとその他の必要なファイルが記録されている。BIOS5は、データ処理装置1の起動時に起動される。また、BIOS5は、ハードディスク10の領域(24)にOS24が格納されていないときに、OS24のインストール処理を行う。

[0168] データ処理装置1において、例えば、アプリケーション25を実行する場合は、オペレータがコマンドを入力し、まず、OS24に対してアプリケーション25の起動指示を行う。データ処理装置1にコマンドが入力されると、制御手段2は、ディレクトリ領域16とFAT14とを参照して当該アプリケーション25の格納されたデータ領域17を特定し、当該データ領域17に記録されたアプリケーション25のプログラムに従って処理を開始する。この場合、制御手段2は必要に応じて、アプリケーション25をメインメモリ3にロードし、処理を実行する。

[0169] そして、アプリケーション25のプログラムに従って、処理結果をディスプレイに表示したり、あるいは、処理結果をハードディスク10に記録する。

他のアプリケーション26やデータクリーニング処理プログラム20を実行する場合も、同様の手順で処理が行われる。

[0170] 次に、データ処理装置1において、ハードディスク10に格納された全てのファイルを削除指定したときのクリーニング処理の課程を図4ー図7を参照して説明する。

データクリーニング処理プログラム20の実行方法は、Windows(当該OS)の他のアプリケーションの実行方法と何ら差異はない。

例えば、図示していないが、本実施形態のデータクリーニング処理プログラム20を実行し易くするために、データクリーニング処理プログラム20のファイル指定アイコン(ショートカットアイコン)を、OSのデスクトップ(表示画面)に配置しておくのが好ましい。

そして、Windowsのファイル一覧機能(エクスプローラ)で表示されるファイル、又は、複数のファイルを包含するフォルダを、マウス等の入力インターフェースでファイル指定アイコンに移動させることにより、移動させたファイルが、クリーニング処理の対象

ファイルに指定されてデータクリーニング処理プログラム20が起動する構成とすることができる。

[0171] 図4において、ハードディスク10に記録された全てのファイルをファイル指定アイコンへ移動させてデータクリーニング処理プログラム20を起動すると、データクリーニング処理プログラム20は、指定されたファイルにOS24及びデータクリーニング処理プログラム20自身が含まれていることを認識する。そして、制御手段2は、データクリーニング処理プログラム20に従って、図5に示すように、クリーニング処理に必要なOS24の一部のファイル24aと、データクリーニング処理プログラム20自身とをメインメモリ3に退避(複写)する。そして、以降の処理をメインメモリ3に退避したデータクリーニング処理プログラム20とOS24aによって続行する。

[0172] 次いで、制御手段2は、メインメモリ3に退避したOS24aを参照し、同じくメインメモリ3に退避したデータクリーニング処理プログラム20に従って、隠し領域23を除く記録領域22内の、OS24及びデータクリーニング処理プログラム20を含む全てのファイルが記録されているハードディスク10の該当するクラスタ(記録領域)に所定データ「00H」を順次上書きする。

[0173] このとき、上書き処理の進行途中に、記録領域22に格納されていたOS24やデータクリーニング処理プログラム20自身が順次上書きされて消去される。しかし、上書き消去される時点では、上書き処理は、メインメモリ3に退避したOS24a及びデータクリーニング処理プログラム20によって行われる。従って、ハードディスク10に格納されたOS24やデータクリーニング処理プログラム20自身が上書き消去されても、上書き処理が中断されてフリーズすることがない。

[0174] 以上の処理により、図6に示すように、ハードディスク10の記録領域22に格納されていた全てのファイルのデータに所定データ「00H」が上書きされてクリーニング処理が完了する。これにより、ハードディスク10の記録領域22は完全に消去され、隠し領域23内のデータだけがそのまま残存する。

[0175] なお、本実施形態では、記録領域22へ「00H」を上書きする構成としたが、「FFH」や「E5H」などの任意のデータを上書きしても良い。また、これら複数のデータを複数回上書きすることにより、残存する不要データの読み取りを、より完全に阻止すること

が可能となる。

[0176] 次いで、図6に示す状態において、データ処理装置1をリセット又は再起動すると、既にハードディスク記録領域22にOS24が存在しないので、制御手段2はBIOS5を起動して、OSのインストールの実行の有無をオペレータに問い合わせる。

なお、データ処理装置1をリセット又は再起動すると、メインメモリ3に退避していたファイル24aやデータクリーニング処理プログラム20は消去される。

[0177] 問い合わせに対して、オペレータがOS24のインストールを指定すると、制御手段2は、隠し領域23に格納されたインストールプログラムを起動し、図7に示すように、OS24をハードディスク10の記録領域22にインストールする。以上の処理により、OS24の再インストールが完了し、ハードディスク10の記録領域22にはOS24だけが格納された状態となる。

[0178] ここで、隠し領域23に、OS24とその他のアプリケーションのインストールプログラムを記録しておくこともできる。このようにすると、OS24とアプリケーションとを再インストールすることができる。再インストール後、オペレータは、直ちにデータ処理装置1を実用することができるようになる。

[0179] このように、本実施形態のデータクリーニング処理プログラム20によれば、ハードディスク10に格納された全てのファイルを指定することにより、隠し領域23のデータ又はプログラムを消去することなく、記録領域22に記録された全てのファイルを上書き消去することができる。又はハードディスク10を、隠し領域23のOS24のインストール機能を用いてOS24だけ(又は、OS24とその他のアプリケーション)がインストールされた初期状態に容易に復元することが可能となる。

[0180] 又、ファイルが記録されていた領域を上書き消去するので、特殊な解析ソフトを用いても元データが復元される恐れがなく、セキュリティを確保することができる。

さらに、本実施形態の構成によれば、隠し領域23にOS24のインストール機能を備えるので、OS24のリカバリーディスクが不要となり、省コスト化を図ることができるうえ、リカバリーディスクの管理が不要である。

[0181] 次に、データ処理装置1において、ハードディスク10に格納されたOS24を除く全てのファイルを指定したときのクリーニング処理を説明する。

図8は、図4のデータ処理装置1において、OS24を除くその他の全てのファイルを指定してデータクリーニング処理を行う課程を示す模式図であり、図9は、図8のデータクリーニング処理が完了した状態を示す模式図である。

[0182] 図4において、記録領域22に記録されたOS24を除き、データクリーニング処理プログラム20を含むその他の全てのファイルをファイル指定アイコンに移動させてデータクリーニング処理プログラム20を起動する。

又は、ファイル指定アイコンをダブルクリックする等の操作でデータクリーニング処理プログラム20を起動する。そして、データクリーニング処理プログラム20のファイル選択メニューからデータクリーニング処理プログラム20を含むその他の全てのファイルを選択する。

[0183] すると、データクリーニング処理プログラム20は、指定されたファイルにデータクリーニング処理プログラム20自身が含まれていることを認識する。そして、制御手段2は、データクリーニング処理プログラム20に従って、図8に示すように、データクリーニング処理プログラム20自身をメインメモリ3に退避(複写)させる。そして、以降の処理をメインメモリ3に退避したデータクリーニング処理プログラム20から実行する。

[0184] 次いで、制御手段2は、記録領域22に格納されたOS24を参照し、メインメモリ3に退避したデータクリーニング処理プログラム20を実行し、OS24を除くデータ領域17のうち、指定したファイルが格納されたクラスタ(記録領域)に、順次所定データ「00H」を上書きする。この場合も、隠し領域23への上書き処理は行われない。

[0185] このとき、上書き処理の進行途中に、データ領域17に格納されたデータクリーニング処理プログラム20が上書き消去される。しかし、上書き消去される時点では、メインメモリ3に退避したデータクリーニング処理プログラム20によって上書き処理が行われているので、ハードディスク10に格納されたデータクリーニング処理プログラム20が上書き消去されても、上書き処理(クリーニング処理)が中断されてフリーズすることはない。

[0186] 制御手段2は、更に、指定したファイル(上書き処理を行ったファイル)をOS24の管理から削除させる。すなわち、OS24でファイルの削除処理を行った場合と同様に、上書き処理を行ったファイルのディレクトリ領域16のデータを削除すると共に、当該フ

ァイルのFAT14，15を開放(「00H」を上書き)する処理を行う。

[0187] 以上の処理により、ハードディスク10のOS24が格納された領域(24)を除くデータ領域17のうち、指定したファイルが格納されていた記録領域に所定データ「00H」が順次上書きされてクリーニング処理が完了する。

データクリーニング処理が完了すると、図9に示すように、ハードディスク10の記録領域21には、OS24だけが格納された記録領域22と隠し領域23とが存在する初期状態に復元される。OS24が存在するので、OS24の再インストールを行う必要はない。

[0188] なお、前記説明では、クリーニング処理の対象のファイルに「00H」を上書きする構成としたが、「FFH」や「E5H」などの任意のデータを上書きしてもよい。単一のデータで複数回上書きしてもよいし、これらのデータを任意に複数個採用して上書きしても良い。

[0189] ところで、OS24を除く他の全てのファイルを指定してデータクリーニング処理を行うと、図9に示すように、依然としてOS24のみが記録領域22に格納されている。従って、データ処理装置1をリセット又は再起動すると直ちにOS24が起動する。

しかし、OS24を構成する多数のファイルは、単体で安定して動作するファイルもあれば、OS24には含まれないデバイスドライバなどと連携して動作するファイルもある。このため、図8，図9し示す処理によって、OS24に含まれないデバイスドライバなどを全て消去すると、OS24の動作が不安定になることがある。

[0190] このような場合は、前記図5，図6に示した手順により、ハードディスク10に格納された全てのファイルを指定して記録領域22のデータを上書き消去した後に、前記図7で示した手順により、隠し領域23のインストール機能を用いてOS24を記録領域22にインストールすれば良い。これにより、OS24の安定した動作を確保することが可能となる。

[0191] 次に、データ処理装置1において、ハードディスク10に格納されたファイルのうち、OS24とデータクリーニング処理プログラム20とを除く他の全てのファイルを指定したときのクリーニング処理を説明する。

図10は、図4のデータ処理装置1において、OS24及び本発明のデータクリーニン

グ処理プログラム20を除く他の全てのファイルを指定してデータクリーニング処理を行う課程を示す模式図であり、図11は図10のデータクリーニング処理が完了した状態を示す模式図である。

[0192] 図4において、ハードディスク10に格納されたOS24とデータクリーニング処理プログラム20を除き、他の全てのアプリケーション20，21及びデータ30，31をファイル指定アイコンに移動させてデータクリーニング処理プログラム20を起動する。すると、データクリーニング処理プログラム20は、指定されたファイルにOS24及びデータクリーニング処理プログラム20の双方が含まれていないことを認識する。

[0193] そして、制御手段2は、メインメモリ3へのファイルの退避を行わずに、記録領域22に格納されたOS24を参照し、データ領域15に格納されたデータクリーニング処理プログラム20に従って、記録領域（データ領域）17のうち、指定したファイルが格納されたクラスタ（記録領域）に、順次所定データ「00H」を上書きする。この場合も、隠し領域23への上書き処理は行われない。

[0194] 制御手段2は、更に、指定したファイル（上書き処理を行ったファイル）をOS24の管理から削除させる。すなわち、OS24でファイルの削除処理を行った場合と同様に、上書き処理を行ったファイルのディレクトリ領域16のデータを削除すると共に、当該ファイルのFAT14，15を開放（「00H」を上書き）する処理を行う。

[0195] 以上の処理により、ハードディスク10のデータ領域17のうち、指定したファイルが格納されていた記録領域に所定データ「00H」が上書きされてクリーニング処理が完了する。

データクリーニング処理が完了すると、図11に示すように、ハードディスク10には、OS24とデータクリーニング処理プログラム20だけが格納された記録領域22と、隠し領域23が存在する状態となる。以上の処理により、ハードディスク10をデータクリーニング処理プログラム20を格納した状態でハードディスク10を初期状態に復元することができる。しかも、OS24の再インストールを行う必要もない。

[0196] なお、前記説明では、データ領域17に「00H」（値）を上書きする構成としたが、「FFH」（値）や「E5H」（値）などの任意のデータを上書きしたり、これら複数のデータを複数回上書きしても良い。

[0197] ところで、図11に示すように、データクリーニング処理によってハードディスク10にOS24とデータクリーニング処理プログラム20だけを残存させると、前記図9で説明した場合と同様に、OS24の動作が不安定になることがある。

[0198] このような場合は、前記したように、ハードディスク10に格納された全てのファイルを指定して記録領域22のデータを上書き消去した後に(図5, 図6参照)、隠し領域23のインストール機能を用いてOS24を記録領域22に再インストールすれば良い(図7参照)。これにより、OS24の安定した動作を確保することが可能となる。

又は、OS24をハードディスク10に残した状態で、OS24を上書きインストールしてもよい。

[0199] 以上、本発明の実施形態を説明したが、本発明のデータクリーニング処理プログラム20が格納されるデータ処理装置1は、前記図4に示した構成に限られるものではない。

すなわち、前記図4の構成では、ハードディスク10の隠し領域23をデータ処理装置1のBIOS5で管理する構成としたが、ハードディスク10に設けられたBIOS(図示せず)で管理する構成を採ることもできる。

[0200] また、隠し領域23をOS(Windows)で管理する構成を採ることも可能である。この構成では、隠し領域23内に格納されたWindows、又は、パーティションで区分されたハードディスク10の別のドライブに格納されたWindowsによって隠し領域23を管理することが可能である。

[0201] また、前記実施形態では、ハードディスク10に隠し領域23を備えた構成として説明したが、隠し領域23を備えていないハードディスク10を用いることも可能である。

ハードディスク10に隠し領域23を備えていない構成であっても、ハードディスク10に格納されたOS24を除く他の全てのファイルを指定してデータクリーニング処理を行うことにより、ハードディスク10のOS24を残存させることができる。従って、ハードディスク10を初期状態に復元して直ちに使用することが可能である。

[0202] 又、ハードディスク10に隠し領域23を備えていない場合には、ハードディスク10に格納された全てのファイルを指定してデータクリーニング処理を行うと、OS24が消去される。従って、OS24を再インストールするためのインストールディスク(リカバリーデ

ィスク)を添付するのが望ましい。

[0203] また、前記実施形態では、ハードディスク10上の全てのファイルを上書き消去する場合や、OS24だけを残して他のファイルを上書き消去する場合、あるいは、OS24とデータクリーニング処理プログラム20を残して他のファイルを全て上書き消去する場合を例に挙げて述べた。しかし、本発明のデータクリーニング処理プログラム20は、OS24だけを上書き消去したり、データクリーニング処理プログラム20だけを上書き消去することも可能である。

[0204] また、前記実施形態では、ハードディスク10(データ記録媒体)に格納されるOS24としてWindowsを例に挙げて説明したが、Windowsの他にもMS−DOSやMacOS、Linuxなどで実施することも可能である。

産業上の利用可能性

[0205] 本発明は、データ記録媒体、又はデータ記録媒体を備えたデータ処理装置を再利用する場合に利用可能である。

請求の範囲

[1] データ記録媒体と、当該データ記録媒体へのアクセス制御を行う制御手段とを備えたデータ処理装置に格納されるデータクリーニング処理プログラムであって、前記データ記録媒体は、ファイルデータを記録する複数のクラスタを有し前記ファイルデータを1又は2以上のクラスタに分散して記録するデータ領域と、前記クラスタを特定するアドレスの付された複数の記録領域を有し、各記録領域に対応するクラスタに記録されたファイルデータに連続するデータの記録されたチェーンクラスタのアドレス又は開放符号のいずれかを各記録領域毎に記録するFAT領域とに区分して前記制御手段で管理され、

前記FAT領域を参照して、開放符号が記録された全ての記録領域のアドレスを抽出し、抽出したアドレスに対応するクラスタに所定データを順次上書きすることを特徴とするデータクリーニング処理プログラム。

[2] データ記録媒体と、当該データ記録媒体へのアクセス制御を行う制御手段とを備えたデータ処理装置に格納されるデータクリーニング処理プログラムであって、前記データ記録媒体は、ファイルデータを記録する複数のクラスタを有し前記ファイルデータを1又は2以上のクラスタに分散して記録するデータ領域と、前記クラスタを特定するアドレスの付された複数の記録領域を有し、各記録領域に対応するクラスタに記録されたファイルデータに連続するデータの記録されたチェーンクラスタのアドレス又は開放符号のいずれかを各記録領域毎に記録するFAT領域とに区分して前記制御手段で管理されると共に、前記データ領域には特定ソフトウェアが格納され、

前記特定ソフトウェアは、データ領域の一部をソフトウェア管理領域として確保すると共に、作成したファイルの保存時には、更新ファイルデータを旧データと区分して前記データ領域に記録し、更に、当該ファイルに係る更新データ及び全ての旧データを記録したクラスタを示すFATデータを前記ソフトウェア管理領域に記録する構成とされ、

前記特定ソフトウェアで作成したファイルを指定し、前記ソフトウェア管理領域に記録されたFATデータを参照して当該ファイルに係るデータの記録された全てのクラスタアドレスを抽出すると共に、前記FAT領域を参照して開放符号が記録された全て

の記録領域のアドレスを抽出し、抽出した双方のアドレスの論理積アドレスに対応するクラスタに所定データを順次上書きすることを特徴とするデータクリーニング処理プログラム。

[3] 前記ソフトウェア管理領域に記録されたFATデータのうち、前記上書き処理が行われたクラスタに対応するFATデータに所定データを上書きすることを特徴とする請求項2に記載のデータクリーニング処理プログラム。

[4] 請求項1に記載のデータクリーニング処理プログラムと請求項2又は3に記載のデータクリーニング処理プログラムの双方の処理機能を備え、前記制御手段によっていずれか一方の処理プログラムを選択的に実行可能なことを特徴とするデータクリーニング処理プログラム。

[5] 前記所定データの上書きは、同一データ又は異なるデータを所定回数だけ繰り返しクラスタに上書きして行うことを特徴とする請求項1乃至4のいずれか1項に記載のデータクリーニング処理プログラム。

[6] 前記データ記録媒体はハードディスクであることを特徴とする請求項1乃至5のいずれか1項に記載のデータクリーニング処理プログラム。

[7] 予め定められた時刻に至ったとき、又は、他の処理が所定時間継続して行われないときに、前記制御手段によって自動的に起動されてクリーニング処理を開始することを特徴とする請求項1乃至6のいずれか1項に記載のデータクリーニング処理プログラム。

[8] データ記録媒体と、オペレーティングシステムによってデータ記録媒体へのアクセス制御を行う制御手段とを備えたデータ処理装置に格納されるデータクリーニング処理プログラムであって、前記データクリーニング処理プログラムはオペレーティングシステム上で動作すると共に、これらのプログラム及びシステムはデータ記録媒体に格納され、

前記データ記録媒体に格納されたファイルを指定すると、指定したファイルに応じて、制御手段によって、クリーニング処理に必要なオペレーティングシステムの一部のファイル又はデータクリーニング処理プログラム自身又はこれらの双方をメインメモリに退避し、データ記録媒体又はメインメモリのオペレーティングシステムを参照しつ

つデータ記録媒体又はメインメモリのデータクリーニング処理プログラムに従って、指定したファイルが格納されていたデータ記録媒体の該当する記録領域に順次所定データを上書きする上書き処理を行うと共に、指定したファイルにオペレーティングシステムが含まれないときは、上書き処理したファイルをオペレーティングシステムの管理から削除させる処理を行うデータクリーニング処理プログラム。

[9] 前記データ記録媒体に格納された全てのファイルを指定可能であり、当該全てのファイルを指定すると、制御手段によって、クリーニング処理に必要なオペレーティングシステムの一部のファイルとデータクリーニング処理プログラム自身とをメインメモリに退避し、メインメモリに退避したオペレーティングシステムを参照しつつ、メインメモリに退避したデータクリーニング処理プログラムに従って前記上書き処理を行うことを特徴とする請求項8に記載のデータクリーニング処理プログラム。

[10] 前記制御手段は、オペレーティングシステムを構成するファイルのプロテクトを解除可能であることを特徴とする請求項9に記載のデータクリーニング処理プログラム。

[11] 前記データ記録媒体に格納されたファイルのうち、前記オペレーティングシステムを除き、データクリーニング処理プログラム又は当該データクリーニング処理プログラムと他のソフトウェア又はデータの少なくともいずれかのファイルを指定可能であり、当該ファイルを指定すると、制御手段によって、データクリーニング処理プログラム自身をメインメモリに退避し、データ記録媒体に格納されたオペレーティングシステムを参照しつつ、メインメモリに退避したデータクリーニング処理プログラムに従って前記上書き処理を行うことを特徴とする請求項8乃至10のうちのいずれかに記載のデータクリーニング処理プログラム。

[12] 前記データ記録媒体に格納されたファイルのうち、前記オペレーティングシステムとデータクリーニング処理プログラムとを除き、他のソフトウェア又はデータの少なくともいずれかのファイルを指定可能であり、当該ファイルを指定すると、制御手段によって、データ記録媒体に格納されたオペレーティングシステムを参照しつつ、データ記録媒体に格納されたデータクリーニング処理プログラムに従って前記上書き処理を行うことを特徴とする請求項8乃至11のうちのいずれかに記載のデータクリーニング処理プログラム。

[13] 前記データ記録媒体は、オペレーティングシステム又はBIOSで管理される隠し領域を備え、当該隠し領域はオペレーティングシステムのインストール機能を備えると共に、前記データクリーニング処理プログラムによる上書き処理が禁止されることを特徴とする請求項8乃至12のうちのいずれかに記載のデータクリーニング処理プログラム。

[14] 前記上書き処理は、同一データ又は異なるデータを所定回数繰り返し上書きして行うことを特徴とする請求項8乃至13のうちのいずれかに記載のデータクリーニング処理プログラム。

[15] 前記データ記録媒体はハードディスクであることを特徴とする請求項8乃至14のうちのいずれかに記載のデータクリーニング処理プログラム。

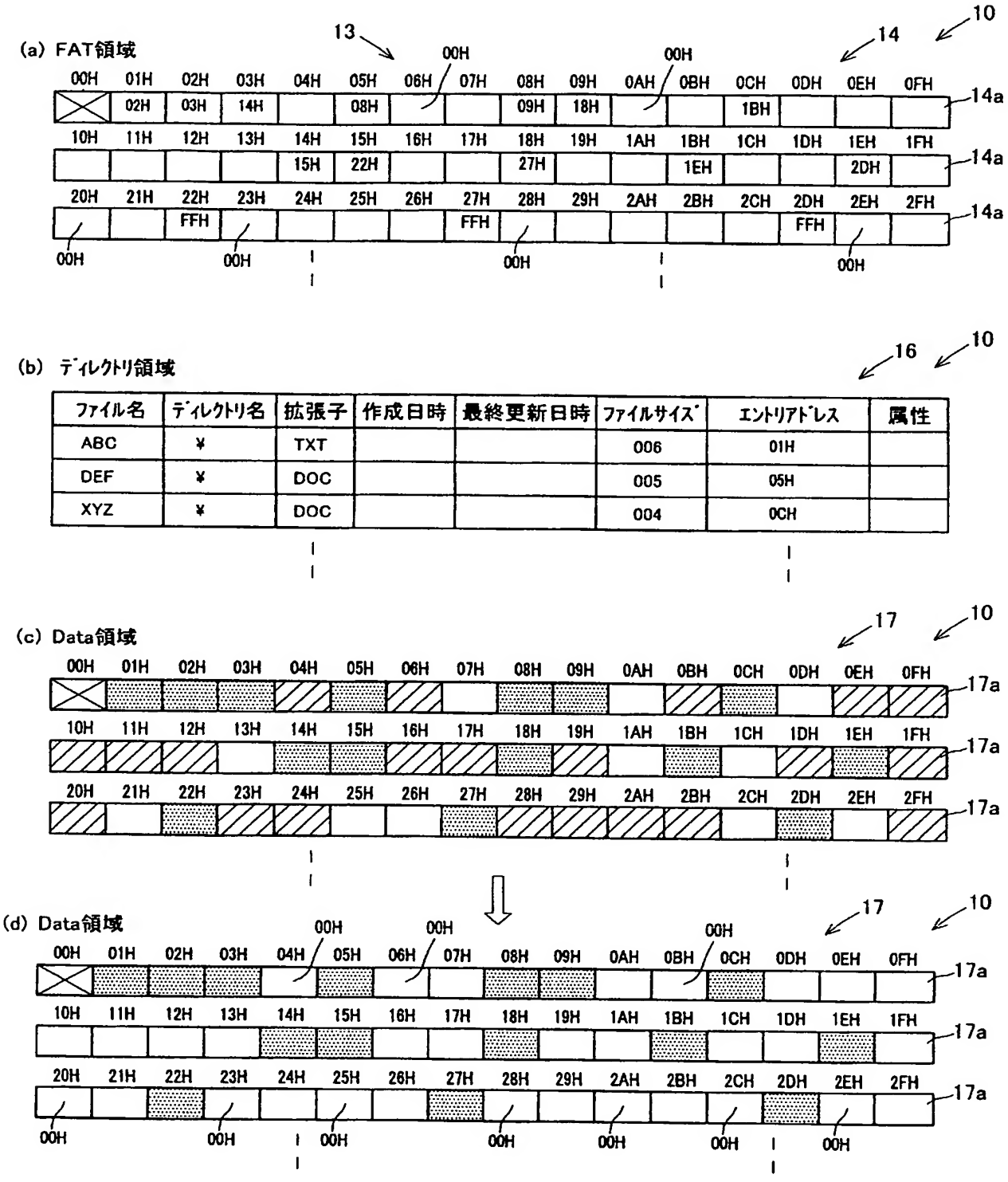
[16] データ処理装置に格納されるデータクリーニング処理プログラムにおいて、前記データ処理装置は、データ記録媒体と、当該データ記録媒体へのアクセス制御を行う制御手段とを備えており、前記データ記録媒体は、データ領域とFAT領域とに区分して前記制御手段で管理されており、前記データ領域は、ファイルデータを記録する複数のクラスタを有し、且つ、前記ファイルデータを1又は2以上のクラスタに分散して記録しており、前記FAT領域は、前記クラスタを特定するアドレスが付された複数の記録領域を有し、且つ、各記録領域に対応するクラスタに記録されたファイルデータに連続するデータが記録されたチェーンクラスタのアドレス又は開放符号のいずれかを各記録領域毎に記録しており、前記FAT領域を参照して、開放符号が記録された全ての記録領域のアドレスを抽出し、抽出したアドレスに対応するクラスタに任意のダミーデータを上書きすることを特徴とするデータクリーニング処理プログラム。

[17] データ処理装置に格納されるデータクリーニング処理プログラムにおいて、前記データ処理装置は、データ記録媒体と、当該データ記録媒体へのアクセス制御を行う制御手段とを備えており、前記データ記録媒体は、データ領域とFAT領域とに区分して前記制御手段で管理されており、前記データ領域は、ファイルデータを記録する複数のクラスタを有し、且つ、前記ファイルデータを1又は2以上のクラスタに分散して記録しており、前記FAT領域は、前記クラスタを特定するアドレスが付された複数の記録領域を有し、且つ、各記録領域に対応するクラスタに記録されたファイルデータ

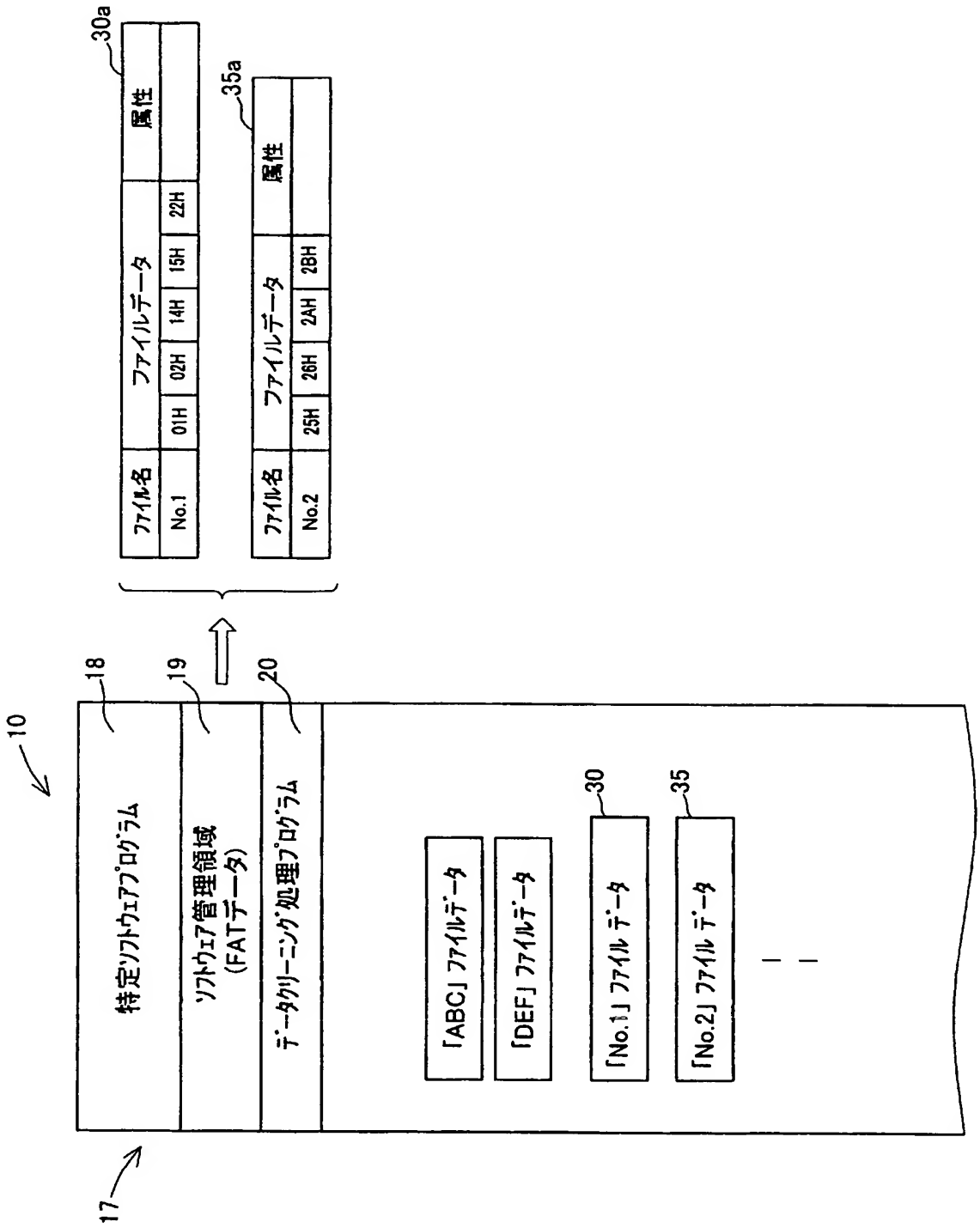
に連続するデータが記録されたチェーンクラスタのアドレス又は開放符号のいずれかを各記録領域毎に記録しており、前記データ領域には特定ソフトウェアが格納されており、前記特定ソフトウェアは、データ領域の一部をソフトウェア管理領域として確保すると共に、作成したファイルデータの保存時には、最新の更新ファイルデータを旧データと区分して前記データ領域に記録し、更に、当該ファイルに係る最新の更新データ及び全ての旧データを記録したクラスタを示すFATデータを前記ソフトウェア管理領域に記録する構成とされ、前記特定ソフトウェアで作成したファイルデータを指定し、前記ソフトウェア管理領域に記録されたFATデータを参照して当該ファイルに係るデータの記録された全てのクラスタアドレスを抽出すると共に、前記FAT領域を参照して開放符号が記録された全ての記録領域のアドレスを抽出し、抽出した双方のアドレスの論理積アドレスに対応するクラスタに任意のダミーデータを上書きすることを特徴とするデータクリーニング処理プログラム。

[18] データ処理装置に格納されるデータクリーニング処理プログラムにおいて、前記データ処理装置は、データ記録媒体と、オペレーティングシステムによって当該データ記録媒体へのアクセス制御を行う制御手段とを備えており、前記データクリーニング処理プログラムはオペレーティングシステム上で動作すると共に、これらのプログラム及びシステムはデータ記録媒体に格納されており、前記データ記録媒体に格納されたファイルをクリーニング処理指定する際に、前記データ処理装置がデータクリーニング処理の途中で停止しないように、データクリーニング処理に必要なオペレーティングシステムの一部のファイル又はデータクリーニング処理プログラム又はこれらの両方をメインメモリに退避させ、メインメモリに退避したデータクリーニング処理に必要なオペレーティングシステムの一部のファイル又はデータクリーニング処理プログラムによってデータクリーニング処理を行うようにしたことを特徴とするデータクリーニング処理プログラム。

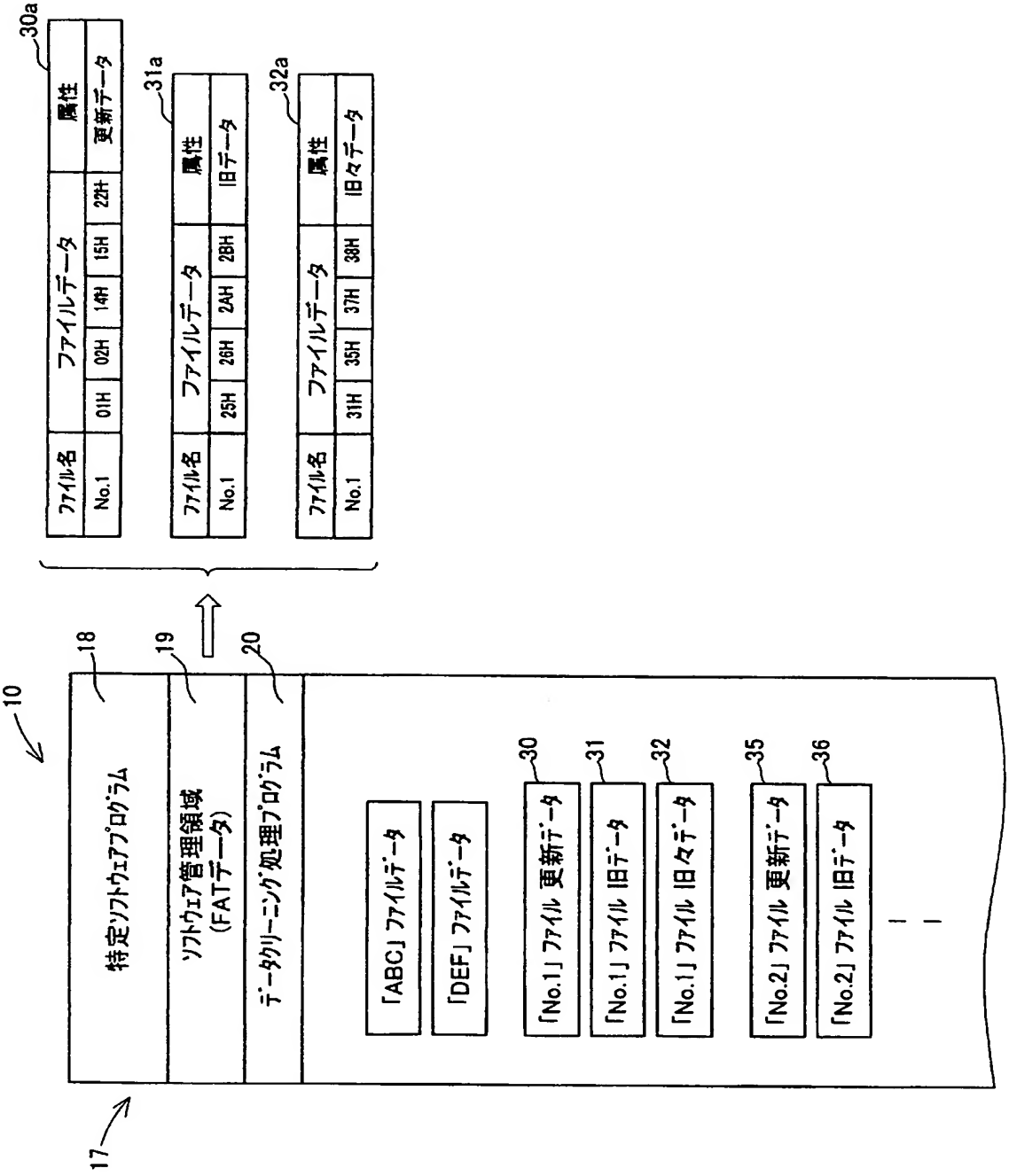
[図1]


(a) FAT領域
13
14
10
00H 01H 02H 03H 04H 05H 06H 07H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH
02H 03H 14H 08H 09H 18H 1BH
10H 11H 12H 13H 14H 15H 16H 17H 18H 19H 1AH 1BH 1CH 1DH 1EH 1FH
15H 22H 27H 1EH 2DH
20H 21H 22H 23H 24H 25H 26H 27H 28H 29H 2AH 2BH 2CH 2DH 2EH 2FH
FFH FFH FFH
14a
(b) ディレクトリ領域
16
10
ファイル名 | ディレクトリ名 | 拡張子 | 作成日時 | 最終更新日時 | ファイルサイズ | エントリアドレス | 属性
ABC | ¥ | TXT | 006 | 01H
DEF | ¥ | DOC | 005 | 05H
XYZ | ¥ | DOC | 004 | 0CH
(c) Data領域
17
10
17a
(d) Data領域

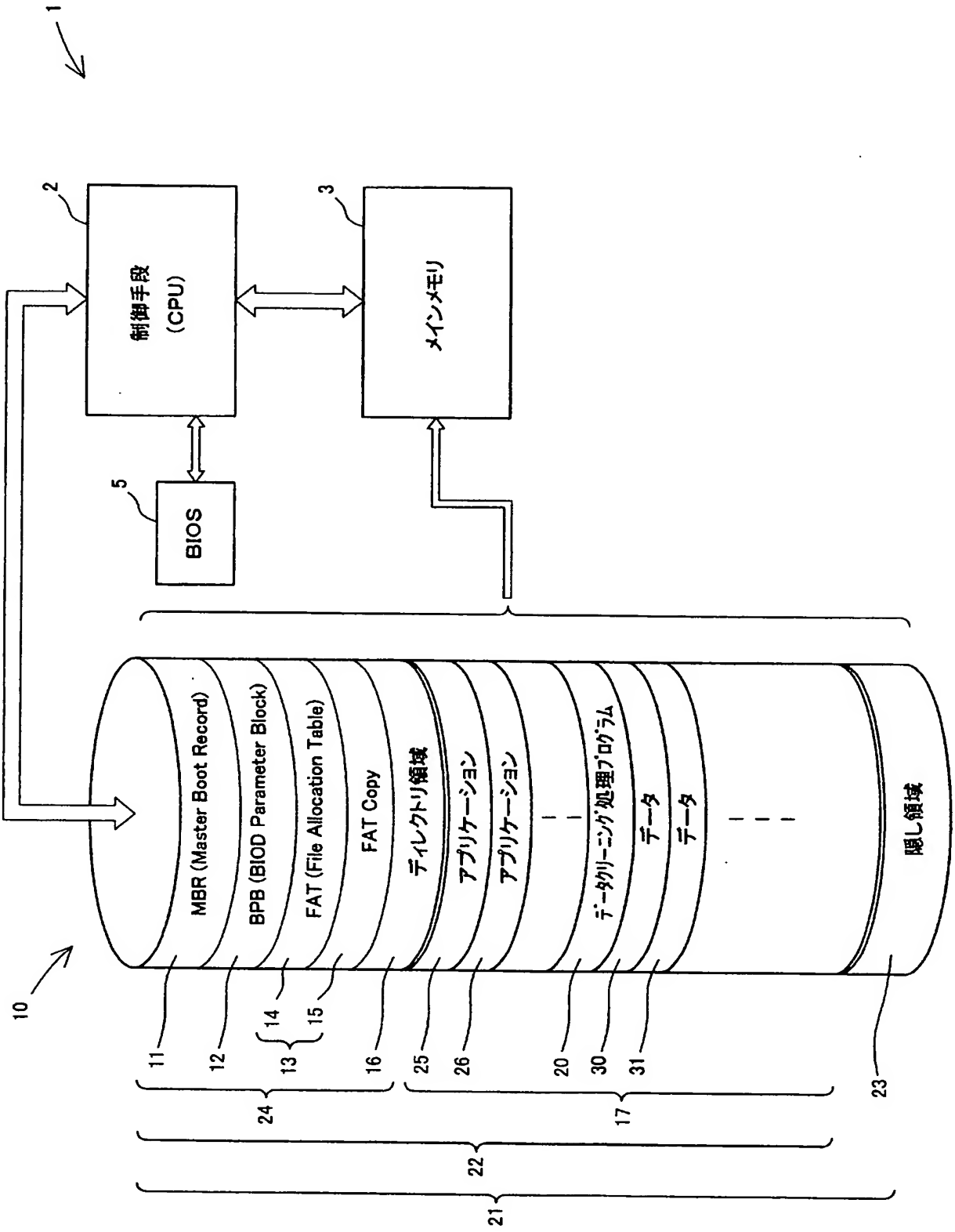
[図2]


30a
ファイル名
ファイルデータ
属性
No.1
01H
02H
14H
15H
22H
35a
ファイル名
ファイルデータ
属性
No.2
25H
26H
2AH
2BH
10
18
19
20
特定ソフトウェアプログラム
ソフトウェア管理領域
(FATデータ)
データクリーニング処理プログラム
「ABC」ファイルデータ
「DEF」ファイルデータ
30
35
「No.1」ファイルデータ
「No.2」ファイルデータ
17

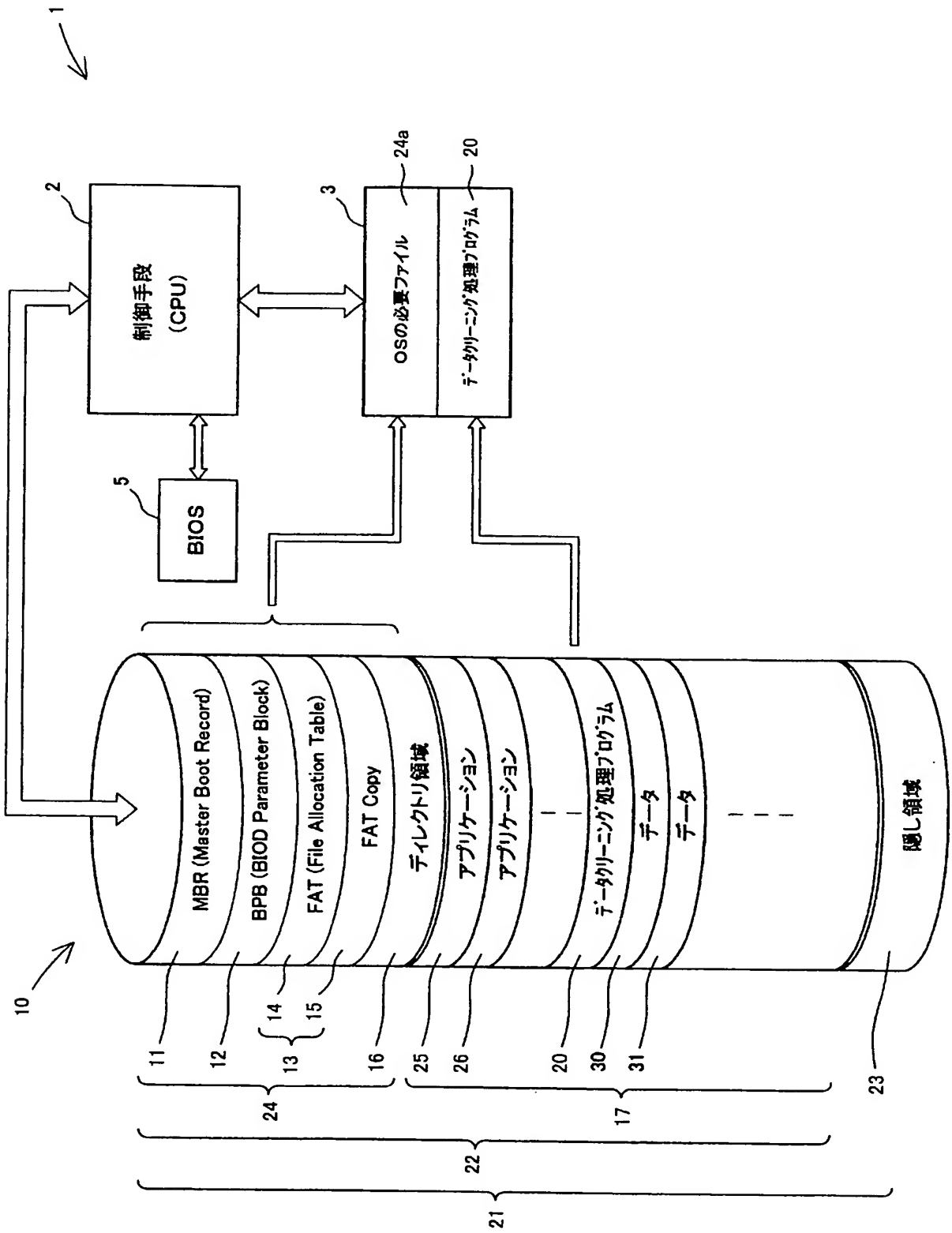
[図3]


30a
31a
32a
ファイル名
ファイルデータ
属性
No.1
01H
02H
14H
15H
22H
更新データ
25H
26H
2AH
2BH
旧データ
31H
35H
37H
38H
旧々データ
10
17
18
19
20
特定ソフトウェアプログラム
ソフトウェア管理領域
(FATデータ)
データクリーニング処理プログラム
「ABC」ファイルデータ
「DEF」ファイルデータ
30
31
32
35
36
「No.1」ファイル 更新データ
「No.1」ファイル 旧データ
「No.1」ファイル 旧々データ
「No.2」ファイル 更新データ
「No.2」ファイル 旧データ

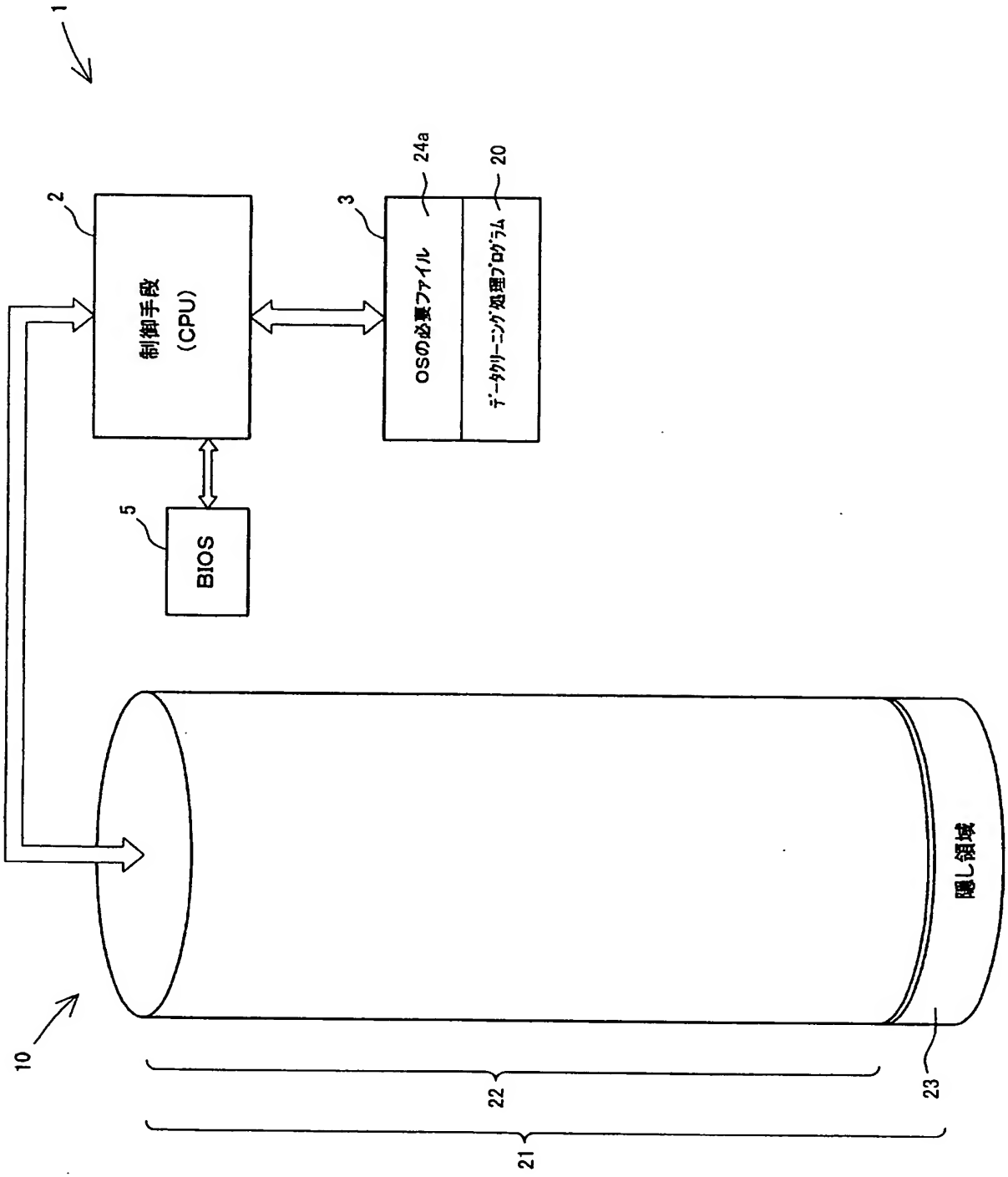
[図4]


1
2
制御手段
(CPU)
3
メインメモリ
5
BIOS
10
MBR (Master Boot Record)
BPB (BIOD Parameter Block)
FAT (File Allocation Table)
FAT Copy
ディレクトリ領域
アプリケーション
アプリケーション
データクリーニング処理プログラム
データ
データ
隠し領域
11
12
13
14
15
16
25
26
20
30
31
23
24
17
22
21

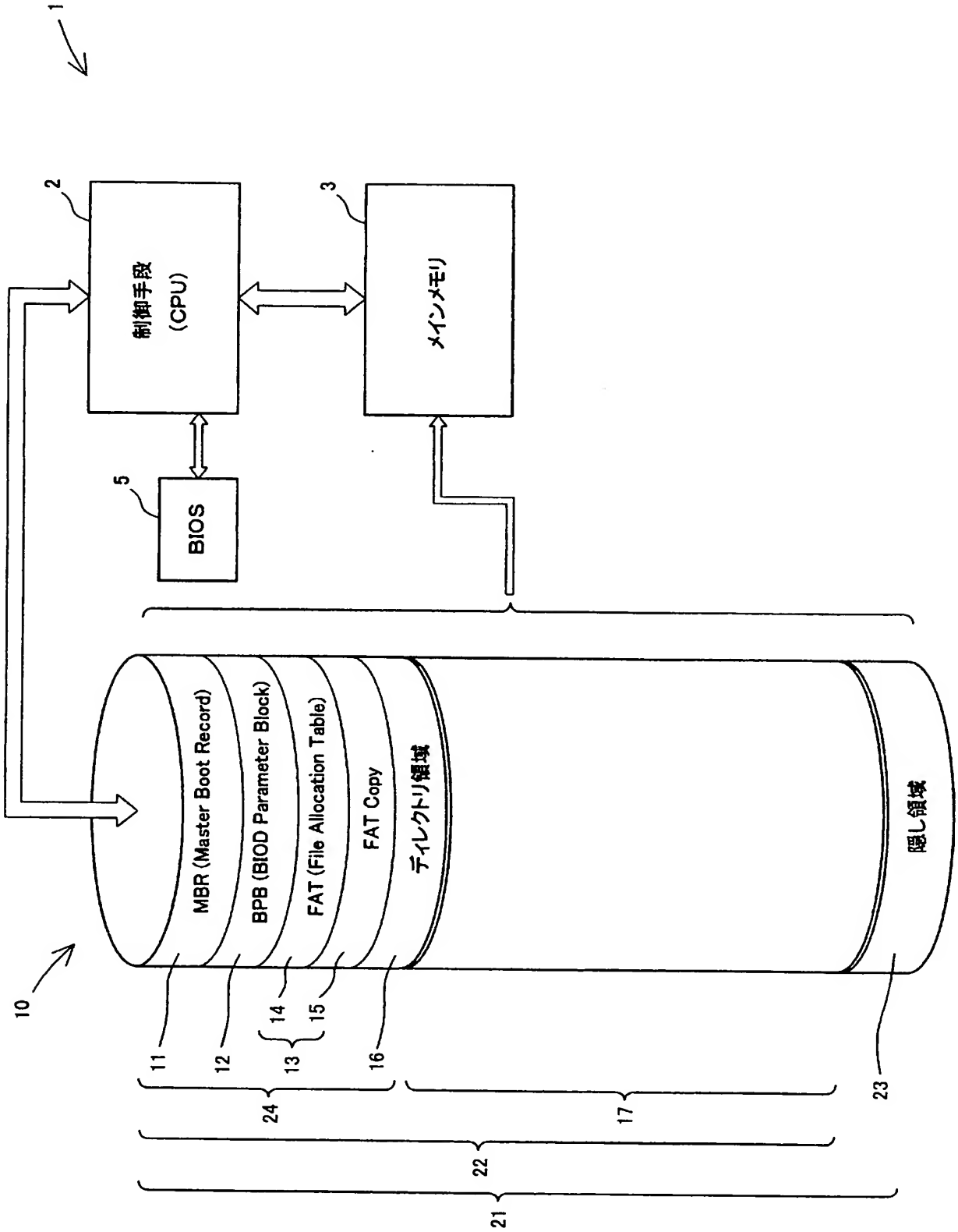
[図5]


1
2
制御手段
(CPU)
3
24a
OSの必要ファイル
20
データクリーニング処理プログラム
5
BIOS
10
MBR (Master Boot Record)
BPB (BIOD Parameter Block)
FAT (File Allocation Table)
FAT Copy
ディレクトリ領域
アプリケーション
アプリケーション
データクリーニング処理プログラム
データ
データ
隠し領域
11
12
13
14
15
16
25
26
20
30
31
23
24
17
22
21

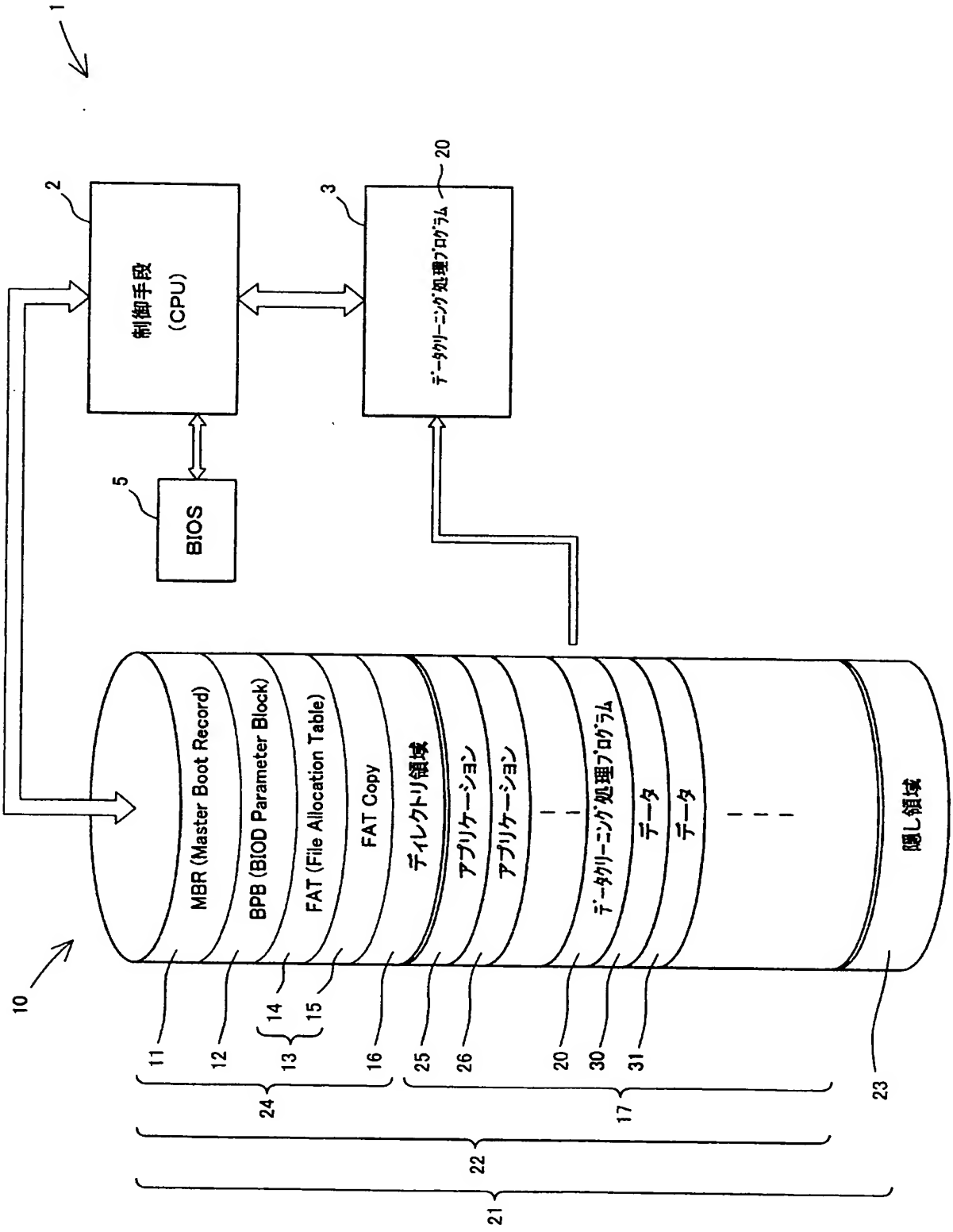
[図6]


1
2
制御手段
(CPU)
3
24a
20
OSの必要ファイル
データクリーニング処理プログラム
5
BIOS
隠し領域
10
22
23
21

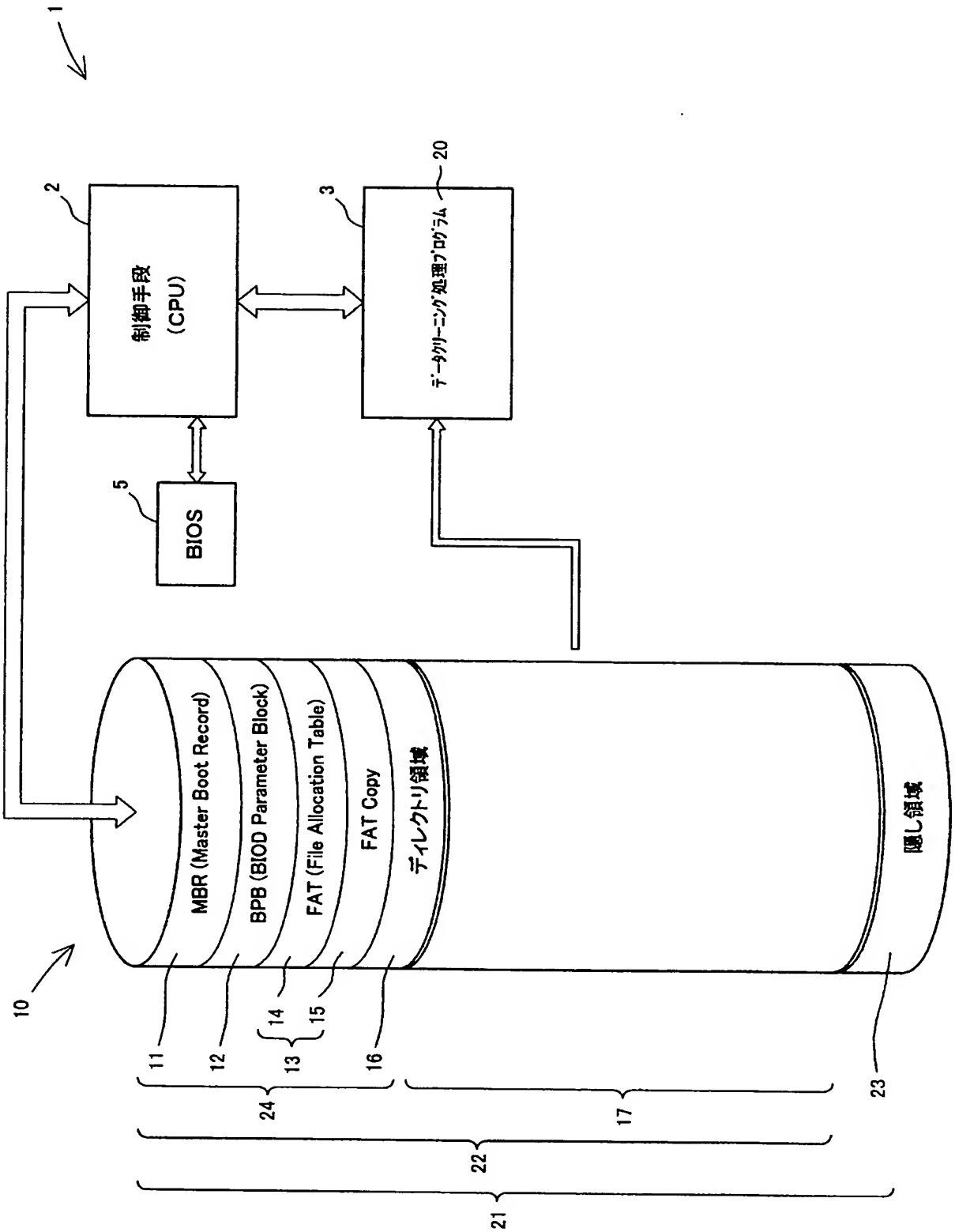
[図7]


1
2
制御手段
(CPU)
3
メインメモリ
5
BIOS
10
MBR (Master Boot Record)
BPB (BIOD Parameter Block)
FAT (File Allocation Table)
FAT Copy
ディレクトリ領域
隠し領域
11
12
13
14
15
16
17
21
22
23
24

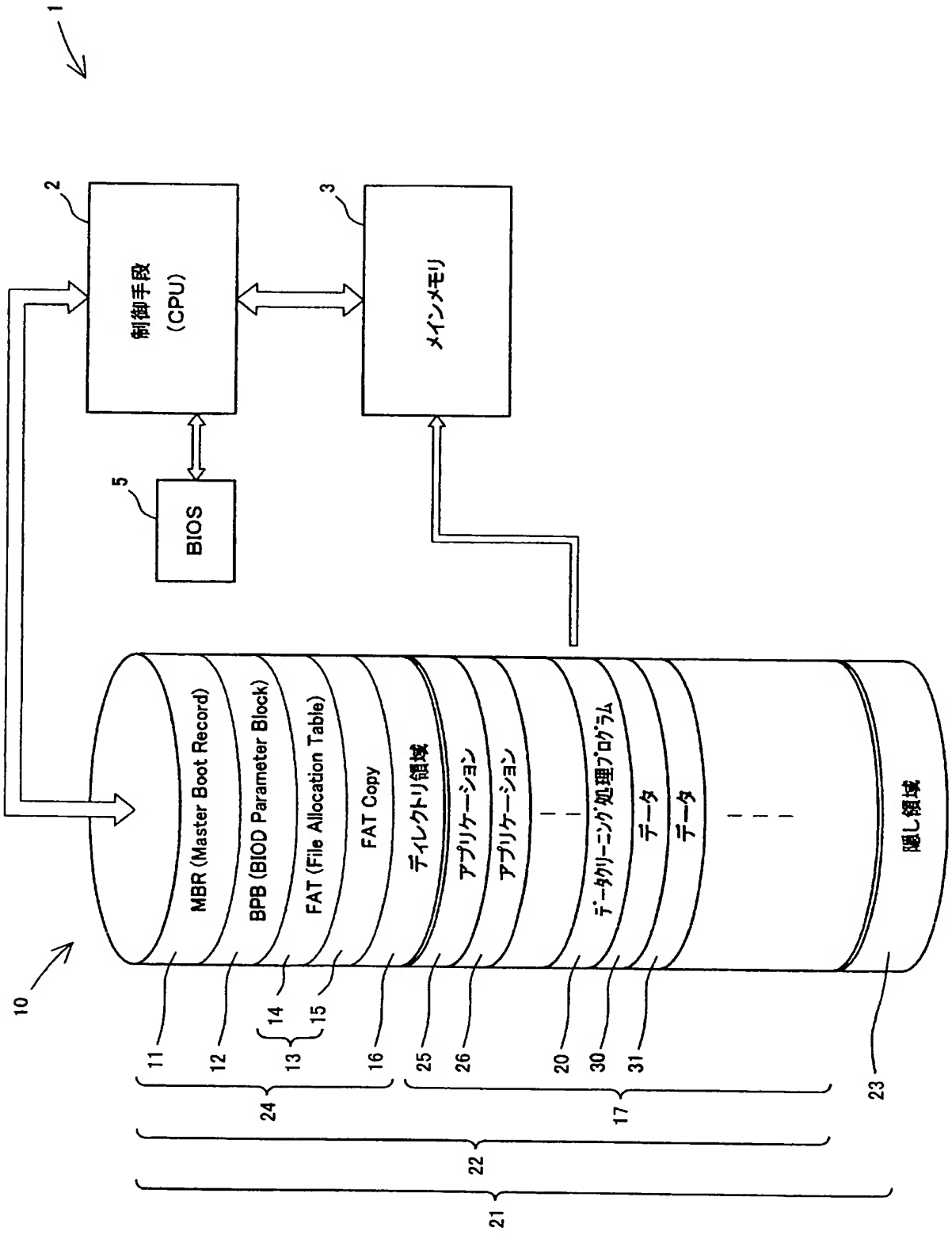
[図8]


1
2
制御手段
(CPU)
3
20
データクリーニング処理プログラム
5
BIOS
10
MBR (Master Boot Record)
BPB (BIOD Parameter Block)
FAT (File Allocation Table)
FAT Copy
ディレクトリ領域
アプリケーション
アプリケーション
データクリーニング処理プログラム
データ
データ
隠し領域
11
12
13
14
15
16
25
26
20
30
31
23
24
17
22
21

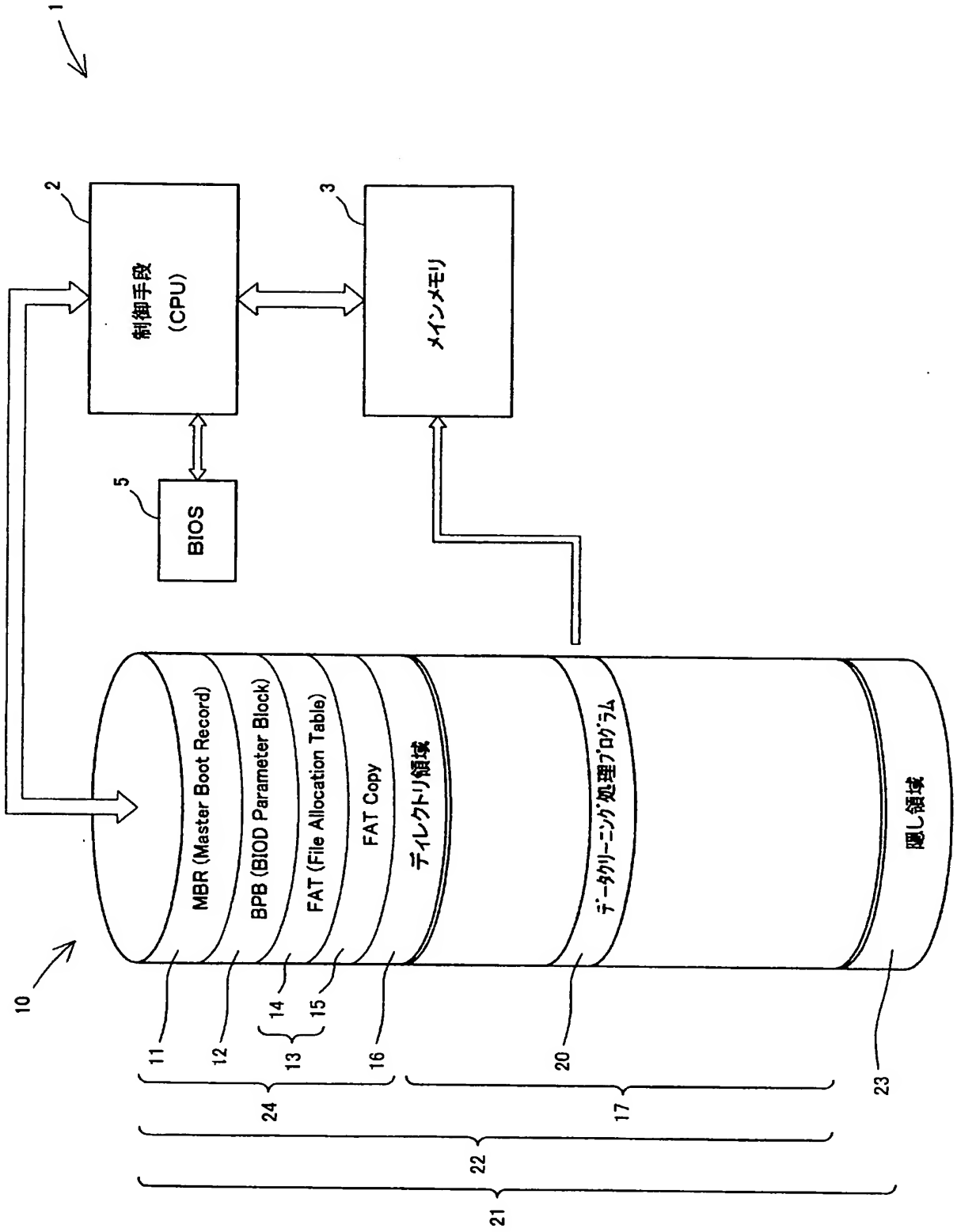
[図9]


1
2
制御手段
(CPU)
3
20
データクリーニング処理プログラム
5
BIOS
MBR (Master Boot Record)
BPB (BIOD Parameter Block)
FAT (File Allocation Table)
FAT Copy
ディレクトリ領域
隠し領域
10
11
12
13
14
15
16
23
24
17
22
21

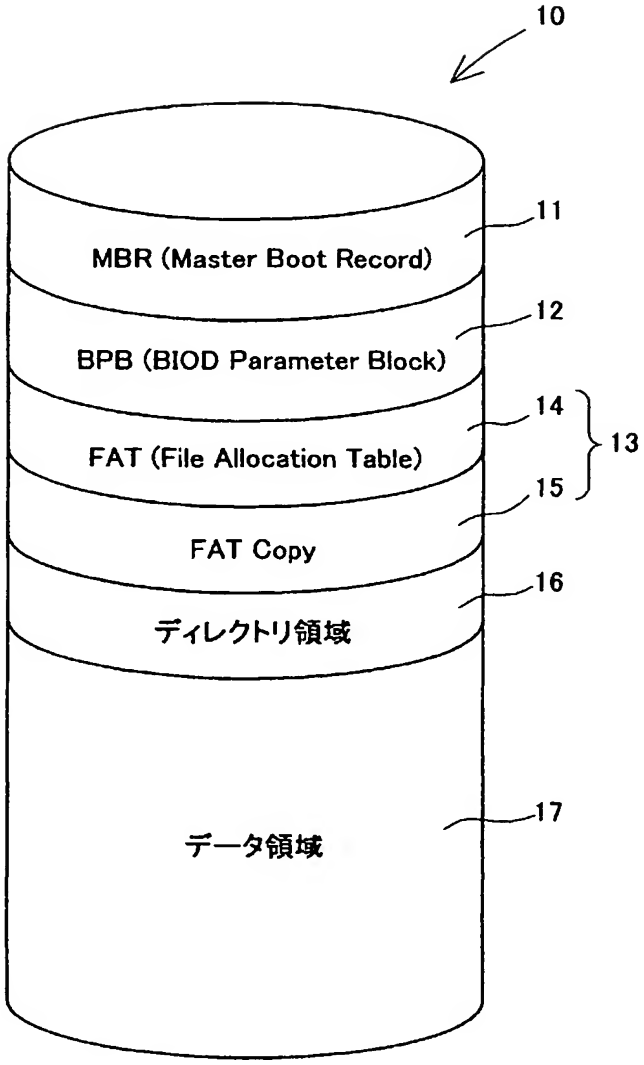
[図10]


1
2
制御手段
(CPU)
3
メインメモリ
5
BIOS
10
MBR (Master Boot Record)
BPB (BIOD Parameter Block)
FAT (File Allocation Table)
FAT Copy
ディレクトリ領域
アプリケーション
アプリケーション
データクリーニング処理プログラム
データ
データ
隠し領域
11
12
13
14
15
16
25
26
20
30
31
23
24
17
22
21

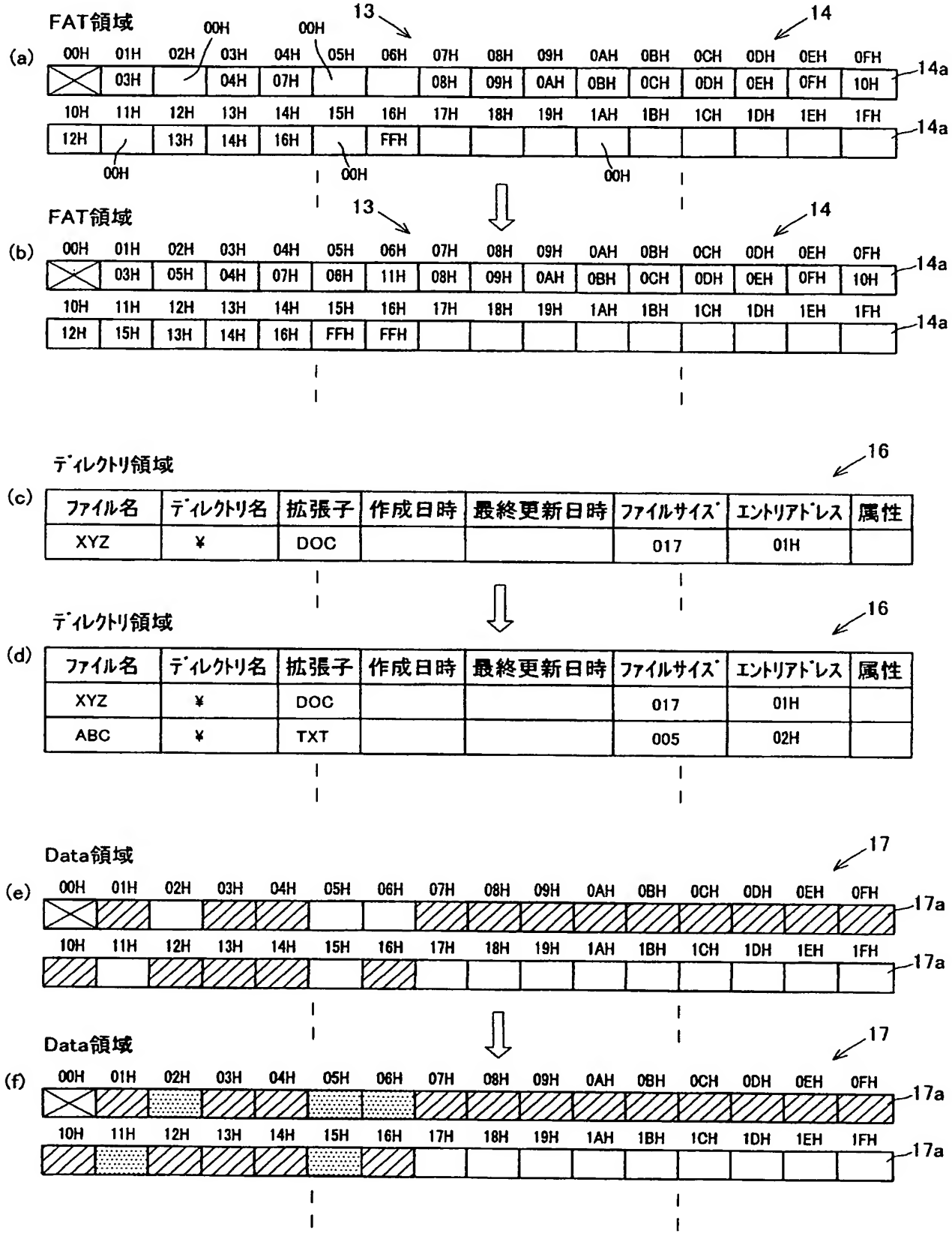
[図11]


1
2
制御手段
(CPU)
3
メインメモリ
5
BIOS
10
MBR (Master Boot Record)
BPB (BIOD Parameter Block)
FAT (File Allocation Table)
FAT Copy
ディレクトリ領域
データクリーニング処理プログラム
隠し領域
11
12
13
14
15
16
20
23
24
17
22
21

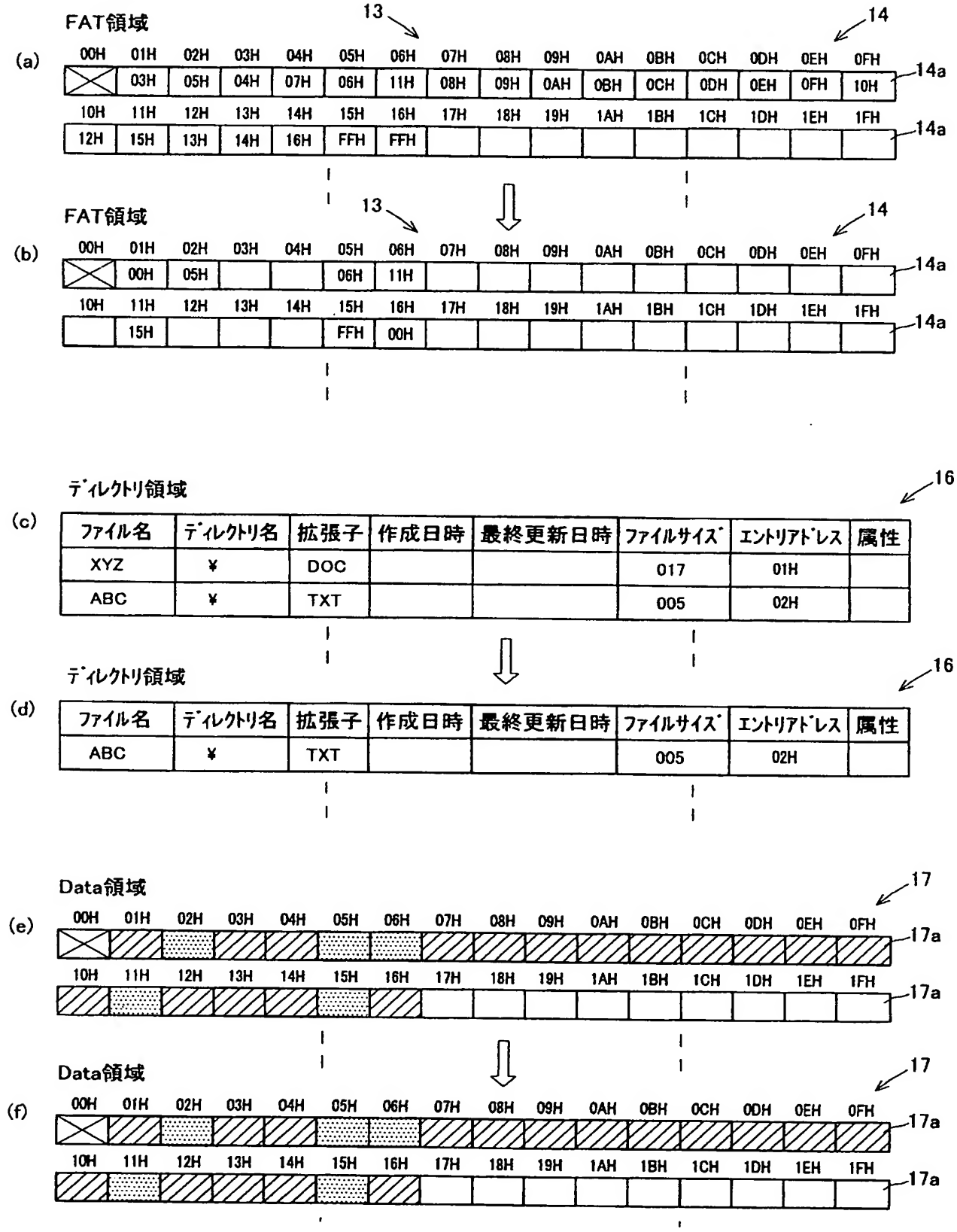
[図12]


10
11
MBR (Master Boot Record)
12
BPB (BIOD Parameter Block)
14
FAT (File Allocation Table)
13
15
FAT Copy
16
ディレクトリ領域
17
データ領域

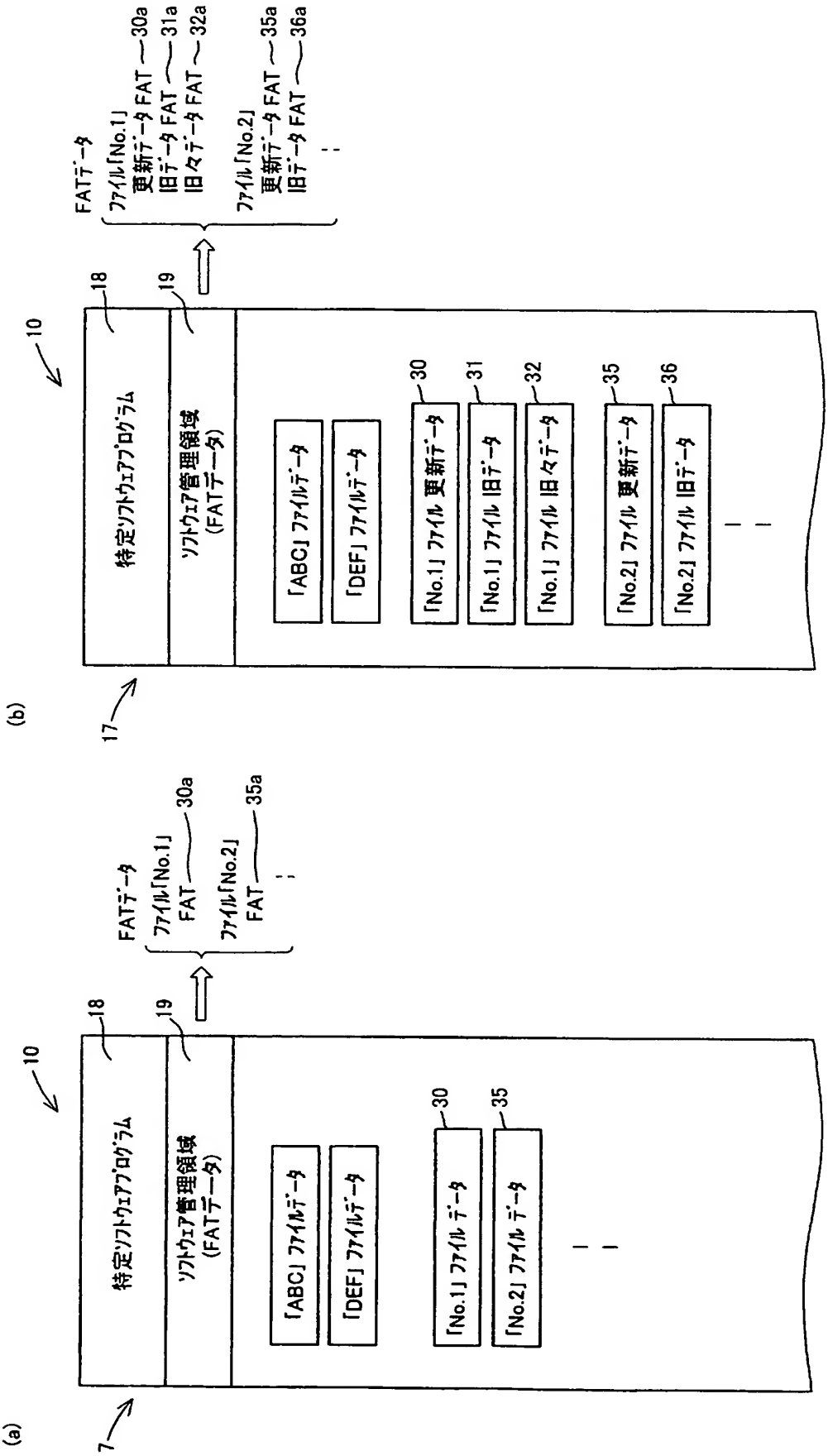
[図13]


FAT領域
13
14
(a)
00H 01H 02H 03H 04H 05H 06H 07H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH
03H 04H 07H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH 10H
14a
10H 11H 12H 13H 14H 15H 16H 17H 18H 19H 1AH 1BH 1CH 1DH 1EH 1FH
12H 13H 14H 16H FFH
14a
00H 00H 00H
FAT領域
13
14
(b)
00H 01H 02H 03H 04H 05H 06H 07H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH
03H 05H 04H 07H 06H 11H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH 10H
14a
10H 11H 12H 13H 14H 15H 16H 17H 18H 19H 1AH 1BH 1CH 1DH 1EH 1FH
12H 15H 13H 14H 16H FFH FFH
14a
ディレクトリ領域
16
(c)
ファイル名 | ディレクトリ名 | 拡張子 | 作成日時 | 最終更新日時 | ファイルサイズ | エントリアドレス | 属性
XYZ | ¥ | DOC | | | 017 | 01H |
ディレクトリ領域
16
(d)
ファイル名 | ディレクトリ名 | 拡張子 | 作成日時 | 最終更新日時 | ファイルサイズ | エントリアドレス | 属性
XYZ | ¥ | DOC | | | 017 | 01H |
ABC | ¥ | TXT | | | 005 | 02H |
Data領域
17
(e)
00H 01H 02H 03H 04H 05H 06H 07H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH
17a
10H 11H 12H 13H 14H 15H 16H 17H 18H 19H 1AH 1BH 1CH 1DH 1EH 1FH
17a
Data領域
17
(f)
00H 01H 02H 03H 04H 05H 06H 07H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH
17a
10H 11H 12H 13H 14H 15H 16H 17H 18H 19H 1AH 1BH 1CH 1DH 1EH 1FH
17a

[図14]


FAT領域
13
14
(a)
00H 01H 02H 03H 04H 05H 06H 07H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH
03H 05H 04H 07H 06H 11H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH 10H
14a
10H 11H 12H 13H 14H 15H 16H 17H 18H 19H 1AH 1BH 1CH 1DH 1EH 1FH
12H 15H 13H 14H 16H FFH FFH
14a
FAT領域
13
14
(b)
00H 01H 02H 03H 04H 05H 06H 07H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH
00H 05H 06H 11H
14a
10H 11H 12H 13H 14H 15H 16H 17H 18H 19H 1AH 1BH 1CH 1DH 1EH 1FH
15H FFH 00H
14a
ディレクトリ領域
16
(c)
ファイル名 | ディレクトリ名 | 拡張子 | 作成日時 | 最終更新日時 | ファイルサイズ | エントリアドレス | 属性
XYZ | ¥ | DOC | | | 017 | 01H |
ABC | ¥ | TXT | | | 005 | 02H |
ディレクトリ領域
16
(d)
ファイル名 | ディレクトリ名 | 拡張子 | 作成日時 | 最終更新日時 | ファイルサイズ | エントリアドレス | 属性
ABC | ¥ | TXT | | | 005 | 02H |
Data領域
17
(e)
00H 01H 02H 03H 04H 05H 06H 07H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH
17a
10H 11H 12H 13H 14H 15H 16H 17H 18H 19H 1AH 1BH 1CH 1DH 1EH 1FH
17a
Data領域
17
(f)
00H 01H 02H 03H 04H 05H 06H 07H 08H 09H 0AH 0BH 0CH 0DH 0EH 0FH
17a
10H 11H 12H 13H 14H 15H 16H 17H 18H 19H 1AH 1BH 1CH 1DH 1EH 1FH
17a

[図15]


(a)
(b)
10
17
18
19
特定ソフトウェアプログラム
ソフトウェア管理領域
(FATデータ)
「ABC」ファイルデータ
「DEF」ファイルデータ
「No.1」ファイル データ
「No.2」ファイル データ
30
35
FATデータ
ファイル「No.1」
FAT
30a
ファイル「No.2」
FAT
35a
「No.1」ファイル 更新データ
「No.1」ファイル 旧データ
「No.1」ファイル 旧々データ
「No.2」ファイル 更新データ
「No.2」ファイル 旧データ
31
32
36
更新データ FAT
旧データ FAT
旧々データ FAT
31a
32a
更新データ FAT
旧データ FAT
35a
36a

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/000664

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06F12/00, G11B20/10, G11B20/12, G11B27/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06F12/00, G11B20/10, G11B20/12, G11B27/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Nobuyuki TAKATA, Handy Reference 50 NORTON UTILITIES Hand book, Natsumesha, 28 April, 1990 (28.04.90), pages 160 to 165	1,5,6,16 7-15,18
Y	Komei HATTORI, Norton Utilities for Macintosh 4.0.4, Mac OS 8.6 perfect guide, Ascii Corp., 01 October, 1999 (01.10.99), pages 114 to 119	7-15,18
Y	Edited by ASCII Shuppankyoku, Hyojun MS-DOS Handbook, first edition, Ascii Corp., 05 October 1985 (05.10.85), pages 117 to 119	8-15,18
Y	Kyosei WATANABE, "Donna Soft Shogai mo 20 Pun de Kaisho suru Client PC no Settei Koseijutsu", Nikkei Windows Pro, 01 December, 2002 (01.12.02), No.69, pages 76 to 83	13

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 25 February, 2005 (25.02.05)	Date of mailing of the international search report 15 March, 2005 (15.03.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/000664

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Makoto SENGOKU, "Haiki Pasokon to Media ga Abunai", Nikkei Byte, 22 May, 2003 (22.05.03), No.241, pages 68 to 73	1-18